

<b>SOLICITATION, OFFER AND AWARD</b>			1. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 7900)		RATING	PAGE 1 OF 1 PAGES
2. CONTRACT NUMBER D13PC00188	3. SOLICITATION NUMBER D13PS00423	4. TYPE OF SOLICITATION <input type="checkbox"/> SEALED BID (IFB) <input checked="" type="checkbox"/> NEGOTIATED (RFP)		5. DATE ISSUED 12/10/2012	6. REQUISITION/PURCHASE NUMBER	
7. ISSUED BY U. S. Department of Interior - IBC - Acquisition Services Directorate 381 Elden Street, Suite 4000, Herndon VA 20170-4817		CODE	8. ADDRESS OFFER TO (If other than item 7) Attn: William Galvin, Contracting Officer			

NOTE: In sealed bid solicitations "offer" and "offeror" mean "bid" and "bidder".

<b>SOLICITATION</b>	
9. Sealed offers in original and <u>5</u> copies for furnishings the supplies or services in the Schedule will be received at the place specified in item 8, or if hand carried, in the depository located in <u>381 Elden Street, Ste. 4,000, Herndon VA 20170</u> until <u>1 pm</u> local time <u>7 January 2013</u> <small>(Hour) (Date)</small>	
CAUTION - LATE Submissions, Modifications, and Withdrawals: See Section L, Provision No. 52.214-7 or 52.215-1. All offers are subject to all terms and conditions contained in this solicitation.	

10. FOR INFORMATION CALL:	A. NAME William Galvin	B. TELEPHONE (NO COLLECT CALLS)		C. E-MAIL ADDRESS william_galvin@nbc.gov
	AREA CODE 703	NUMBER 964	EXT. 3690	

11. TABLE OF CONTENTS							
(X)	SEC.	DESCRIPTION	PAGE(S)	(X)	SEC.	DESCRIPTION	PAGE(S)
PART I - THE SCHEDULE				PART II - CONTRACT CLAUSES			
X	A	SOLICITATION/CONTRACT FORM		X	I	CONTRACT CLAUSES	
X	B	SUPPLIES OR SERVICES AND PRICES/COSTS		PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACH.			
X	C	DESCRIPTION/SPECS./WORK STATEMENT		X	J	LIST OF ATTACHMENTS	
X	D	PACKAGING AND MARKING		PART IV - REPRESENTATIONS AND INSTRUCTIONS			
X	E	INSPECTION AND ACCEPTANCE			K	REPRESENTATIONS, CERTIFICATIONS AND OTHER STATEMENTS OF OFFERORS	
X	F	DELIVERIES OR PERFORMANCE				L	INSTRS., CONDS., AND NOTICES TO OFFERORS
X	G	CONTRACT ADMINISTRATION DATA			M	EVALUATION FACTORS FOR AWARD	
X	H	SPECIAL CONTRACT REQUIREMENTS					

**OFFER (Must be fully completed by offeror)**

NOTE: Item 12 does not apply if the solicitation includes the provisions at 52.214-16, Minimum Bid Acceptance Period.

12. In compliance with the above, the undersigned agrees, if this offer is accepted within 180 calendar days (60 calendar days unless a different period is inserted by the offeror) from the date for receipt of offers specified above, to furnish any or all items upon which prices are offered at the set opposite each item, delivered at the designated point(s), within the time specified in the schedule.

13. DISCOUNT FOR PROMPT PAYMENT <small>(See Section I, Clause No. 52.232-8)</small>	10 CALENDAR DAYS (%) 0	20 CALENDAR DAYS (%) 0	30 CALENDAR DAYS (%) 0	CALENDAR DAYS (%) 0
14. ACKNOWLEDGMENT OF AMENDMENTS <small>(The offeror acknowledges receipt of amendments to the SOLICITATION for offerors and related documents numbered and dated):</small>	AMENDMENT NO.		DATE	
	0001		12/14/2012	
	0002		12/17/2012	

15A. NAME AND ADDRESS OF OFFEROR	CODE	088192141	FACILITY	16. NAME AND THE TITLE OF PERSON AUTHORIZED TO SIGN OFFER <small>(Type or print)</small> Kerry Mooney President, Federal Division
	ValueOptions, Inc. 240 Corporate Boulevard Norfolk, VA 23502			
15B. TELEPHONE NUMBER		<input type="checkbox"/> 15C. CHECK IF REMITTANCE ADDRESS IS DIFFERENT FROM ABOVE - ENTER SUCH ADDRESS IN SCHEDULE.	17. SIGNATURE <i>Kerry Mooney</i>	18. OFFER DATE 1/31/13
AREA CODE 757	NUMBER 459			

**AWARD (To be completed by Government)**

19. ACCEPTED AS TO ITEMS		20. AMOUNT 78,934,935.2	21. ACCOUNTING AND APPROPRIATION	
22. AUTHORITY FOR USING OTHER THAN FULL OPEN COMPETITION: <input type="checkbox"/> 10 U.S.C. 2304 (c) <input checked="" type="checkbox"/> 41 U.S.C. 253 (c)			23. SUBMIT INVOICES TO ADDRESS SHOWN IN <small>(4 copies unless otherwise specified)</small>	
24. ADMINISTERED BY (If other than item 7)			25. PAYMENT WILL BE MADE BY Reference Section G	
26. NAME OF CONTRACTING OFFICER (Type or print) William Galvin			28. AWARD DATE 31 Jan 2013	
			27. UNITED STATES OF AMERICA <i>William Galvin</i> <small>(Signature of Contracting Officer)</small>	

IMPORTANT - Award will be made on this Form, or on Standard Form 26, or by other authorized official written notice.

AUTHORIZED FOR LOCAL REPRODUCTION  
Previous edition is unusable

STANDARD FORM 33 (REV., 9-97)  
Prescribed by GSA - Far (48 CFR) 53.214 (c)

## **SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS**

This Contract is issued by following the guidelines of Federal Acquisition Regulation (FAR) Part 12 (“Acquisition of Commercial Items”) and FAR Part 15 (“Contracting by Negotiation”) and various other FAR Sections as applicable. The Offeror’s Final Proposal Revision (FPR) dated 18 January 2013 is hereby incorporated in its entirety as fully set forth herein. In the event of a conflict between the FPR and the Award Documents, the Award Documents shall supersede.

The North American Industry Classification (NAICS) Code is 624190 (Other Individual and Family Services), business size standard of \$7.0 Million in annual receipts.

### **CCR Registration**

The Offeror must be registered with the Central Contractor Registration ([www.ccr.gov](http://www.ccr.gov)), or its replacement System for Award Management, [www.sam.gov/portal/public/SAM/](http://www.sam.gov/portal/public/SAM/).

### **Contracting Officer and Contact Information for Inquiries**

The Contracting Officer (CO) for this requirement is William Galvin. All questions regarding this Contract must be submitted via e-mail to [William\\_Galvin@nbc.gov](mailto:William_Galvin@nbc.gov) and [Christopher S Morningstar@nbc.gov](mailto:Christopher_S_Morningstar@nbc.gov).

## **SECTION B – SUPPLIES OR SERVICES AND PRICES**

### **B.1 Consideration and Payment**

B.1.1 The award is a hybrid contract comprised of mostly firm-fixed priced CLINs with some time and material CLINs.

B.1.2 The price of this effort is in accordance with the CLIN structure (reference Section J, Attachment 1).

B.1.2.1 Definition: CLIN 0001 Tiers 1-11. The tier system outlined in CLIN 0001 is designed to allow the Government and the contractor to establish a base level of operation aligning expected call volumes with contractor staffing, and to move between tiers to accommodate increased/decreased call volumes. The Offeror shall invoice the firm fixed price for the tier corresponding to the actual call volume experienced each month.

B.1.2.2 Definition: CLIN 0010 Transition Out (Optional). The Government will exercise this Optional CLIN in the event that the MOS Program is awarded to a different Vendor. Since it is undetermined when the competitive contract will be awarded, this optional CLIN may be carried forward to any future period of performance (including option periods) within this contract.

### **B.2 Other Direct Costs (ODCs)**

The CO shall determine the allowability of ODCs in accordance with FAR Subpart 31.2. The Offeror shall present a detailed list of all ODC items (excluding profit), item pricing, and a basis of estimate for each price. The Offeror shall list all ODCs needed to perform services described in the Performance Work Statement (PWS).

### **B.3 Travel**

All travel must be approved in advance, in writing, by the Contracting Officer Representative (COR) prior to travel. Once approved, the contractor shall be reimbursed for the actual costs of transportation, lodging, meals, and incidental expenses during the authorized travel IAW FAR 31.205-46, which incorporates the Federal Travel Regulations (FTR). Current Per Diem rates can be accessed electronically at <http://www.defensetravel.dod.mil/site/perdiem.cfm>.

## **SECTION C – DESCRIPTIONS AND SPECIFICATIONS**

### **PERFORMANCE WORK STATEMENT (PWS) MILITARY COMMUNITY AND FAMILY SUPPORT SERVICES MILITARY ONESOURCE PROGRAM**

#### **1.0 SCOPE**

##### **1.1 INTRODUCTION**

On behalf of the Military Departments and the Guard and Reserve Components, the Department of Defense (DoD) requires a Contractor to provide services in support of the Military OneSource (MOS) Program. This program, a primary source of information for troops and families, provides members of the Armed Forces and their families, about 6 million persons (“Client”) at locations worldwide, with a broad array of information and referrals to both military and civilian resources as well as counseling services. Over the course of this contract, the DoD may also designate other civilian personnel to be Clients.

(i) These services shall be available 24 hours a day, 7 days a week (24/7), through the Internet, telephone (via 800 number and collect calls) e-mail, postal, and face-to-face counseling is provided upon request. The Contractor shall maintain the current 800 number and be responsible for all costs associated with the toll free services including service provider fees and usage charges.

(ii) This is a dynamic environment encompassing comprehensive support systems related to military members and their families. Unpredictable world events (such as natural or man-made disasters) and military situations (such as unscheduled deployments) may affect this contract, thus challenging DoD and the Contractor with developing innovative options and solutions to support military members and their families in a “just-in-time” mode.

##### **1.1.1 BACKGROUND**

In recent history, U.S. military forces have been continuously engaged in armed conflicts and humanitarian assistance missions around the world. Ongoing deployments, changing demographics, and other challenges exert considerable stress on military members and their families. Unnecessary concern over these and other issues can diminish mission readiness, particularly for those on the battlefield. There is every reason to believe this operational tempo will exist for the foreseeable future.

These deployments into harm’s way have placed extreme stress on military families. Military families are struggling to balance complex and competing demands requiring a wide range of problem solving skills to include, but not limited to: single parenting; communications; child care; financial stability; spouse employment; fluctuating family income; frequent relocations; isolation from other military families (Guard and Reserve families); family’s education needs, etc. The DoD recognizes that families also serve and is committed to supporting them. The Department intends to make expert telephonic consultation, referral, and information services and short term, situational, problem-solving counseling services available to troops and their families, on demand.

The DoD recognizes the reciprocal relationship that binds the military member, the military mission, and military families. MOS demonstrates the commitment of the DoD to improving the quality of life for military members and their families. These information and support services, fully integrated with other resources available throughout the military community, reveal the concern of military leaders for the welfare of military members and their families. MOS helps ensure that military members will continue to be mission deployable.

#### **1.2 SCOPE OF WORK**

The scope of the MOS effort encompasses all resources and development of resources, processes, personnel, materials, training, equipment, and technology necessary to provide service members and their families with unlimited access (via 24/7, toll-free telephone and on-line/Internet) to stateside and international information, referral and counseling services available through a centralized source.

1.2.1 Individuals are eligible to be MOS Clients if they are (reference Section J, Attachment 2):

- Active duty members of the Military Services (Army, Navy, Marine Corps, and Air Force) and their legal dependents;
- Members of the Army Guard, Air Guard, the Army, Navy, Marine Corps, and Air Force Reserves, and their legal dependents;
- Members of the US Coast Guard on active duty, and their legal dependents, mobilized under the authority of the DoD; and
- DoD Civilians staffing military support programs as identified by DoD, to include Chaplains, Family Support Services Staff, medical personnel and DoD Education Activity staff (approximately 50,000 staff members).
- Members of the DoD Civilian Expeditionary Work Force and their legal dependents.

1.2.2 The MOS Program includes, but is not limited to: call center operations providing expert information/referral and educational/consultation services; educational/information materials; non-medical counseling services; the Joint Family Support Assistance Program (JFSAP), and Spouse Education and Career Opportunities (SECO). The SECO program is to transition (not-to-exceed 90 days) to the new SECO provider. Information/referrals and education/consultation services shall cover the full range of quality of life services/programs in both the military and civilian sectors. Services shall be provided both in the Continental United States (CONUS) and Outside the Continental United States (OCONUS), with the exception of face-to-face non-medical counseling, which is only available within CONUS.

1.2.3 The scope of MOS provides professional and technical expertise, as required, in a variety of disciplines that impact the lives of military members and their families. The counselors/consultants shall be available 24/7, to provide expert consultation, education, information, and referral services. These services shall be consultative in nature; solicitation of any type is prohibited under this contract (reference Section J, Attachment 14).

1.2.4 The Contractor shall maintain an Employee Assistance Professional/Work Life structural organization and integrate non-medical counseling services within MOS.

1.2.5 It is a minimum requirement that anyone working on the MOS Program must be a U.S. Citizen.

## **2.0 APPLICABLE DOCUMENTS AND REFERENCES**

Information sources used for program and content development will be from official Government Sources or authorized affiliates. Internet domains .gov, mil, and .edu, are the primary resource sources. Refer to Section J, Attachment 11, for mandatory compliance requirements of this PWS.

Also, reference Section J, Attachment 3 for a Glossary of Terms and Section J, Attachment 8 for a listing of Acronyms/Symbols.

## **3.0 MOS PROGRAM REQUIREMENTS**

The Contractor shall provide call center services necessary to manage and operate DoD's MOS Program, 24/7. Call centers shall be located in CONUS. Services shall include recruiting, hiring, training and managing a professional staff, maximizing the use of military spouses, wounded warriors, and veterans to provide expert consultation and education on a wide array of topics; the establishment of business applications; interpreter and translation services; back-up operations and surge handling; developing the technological infrastructure necessary to operate a call center; and refreshing the technology used to maintain it state-of-the-art. Information and referral services provided include but are not limited to:

Child Care (referrals to Child Care Aware only; no additional information shall be provided)
Counseling for Non-Medical Issues (telephonic, on-line, in-person)
Deployment Support (mobilization and reintegration)
Disability
Domestic Violence prevention
Elder Care
Education Services for Adults, Children and Youth (DODEA, Tuition Assistance, K-12)
Everyday Issues (e.g., location of a plumber or car repair)
Family Support (Active Duty, Guard and Reserve )
Financial Matters (budgeting, financial counseling and planning, on-line state and federal tax filing and assistance, debt reduction, etc.)
Health and Wellness
Housing (rentals, mortgage, military housing allowances)
Legal Services Information
Lodging in military facilities
Military Benefits
Parenting
Pet Care
Recreation (i.e. Morale, Welfare)
Relocation
Single Troop Services
Shopping and Services (Commissary and Post Exchanges)
Special Needs Services for Children and Adults
Spouse Education and Career Counseling
State Support to the Guard and Reserve
Substance Abuse (addiction, recovery, etc.)
Transition to Civilian Life
TRICARE – Military Health Care Services Referral
Wounded Warrior Support (Health and Benefits Referral)
Youth Services

Additional troop and family assistance will be provided as identified by the DoD.

#### **4.0 MISSION REQUIREMENTS**

##### **MISSION EXECUTION TASKS**

##### **TASK 1 CALL CENTER OPERATIONS, INFORMATION TECHNOLOGY (IT) AND INFORMATION ASSURANCE (IA) SERVICES, CASE MANAGEMENT, REPORTS, DISASTER CONTINUITY OF SERVICES, AND MILITARY UNIQUE REQUIREMENTS**

#### **4.1 MOS CALL CENTER OBJECTIVE**

To encompass all resources and development of resources, processes, personnel, materials, training, equipment, and technology necessary to provide Service members and their families with unlimited access (via 24/7, toll-free telephone and on-line/Internet) to stateside and international information, referral and counseling services available through a centralized source.

#### 4.1.1 MOS CALL CENTER MINIMUM REQUIREMENTS

The Contractor shall provide staff, processes, procedures, and the technological infrastructure necessary to operate a 24/7 toll free MOS Call Center. One call center shall be physically located in the National Capital Region (NCR).

4.1.1.1 The Call Center consultants answering the telephones shall have a minimum of a master's degree in social work or other human services fields, and a minimum of three years recent and relevant practical experience, and reflect the ethnic and cultural diversity of the military community.

4.1.1.2 The Contractor will ensure that a single number can be used by Service members and their families from any location world-wide to access the MOS Call Center. The Contractor's technical infrastructure provides back up call center capability instantaneously. The Call Center service shall include redundant back-up call centers with trained and experienced personnel and technical support capable of supporting toll-free stateside and international calls from MOS Clients. There is a minimum of two call centers for this requirement. One must be in a geographic location unlikely to be affected by a natural/man-made disaster in the other. The Contractor shall provide the ability of OCONUS callers to access country specific numbers for both toll free and collect calls, which shall be available on the MOS webpage.

4.1.1.3 Upon successful transition of the SECO program to the new SECO program provider, the Call Center triage consultants will answer calls for SECO, which, including the SECO Career Center, is provided under a separate contract. If a caller is determined to be a military spouse calling for education or career information or counseling, or is calling for information regarding the My Career Advancement Account (MyCAA) Program or Military Spouse Employment Partnership (MSEP) Program, the call will be transferred to a SECO Career Center counselor, via warm hand-off, during SECO Career Center regular operating hours of seven am until ten pm (7am-10pm) eastern time Monday through Friday and from ten am until five pm (10am-5pm) eastern time on Saturday. The MOS triage consultant will enter caller's information in the MOS Contractor's CMS (for call accountability purposes only) and initiate a warm handoff to the SECO Career Center staff.

4.1.1.4 For calls received from a military spouse for SECO, MyCAA, or MSEP outside of the SECO Career Center operating hours, MOS triage consultants will take a message and log the message in a queue to be returned by the SECO Career Center staff within the next three business days.

4.1.1.5 For calls received from a MyCAA School representative, MSEP Partner or corporation, MOS triage consultants will provide a warm hand off and a telephone number, which will be provided by the Government, to the SECO MyCAA School liaison team or the SECO MSEP Partner liaison team. For calls received outside of the SECO Career Center operating hours, MOS triage consultants will take a message and log the message in a queue to be returned by the SECO Career Center staff within the next three business days.

4.1.1.6 The Contractor shall provide on a monthly basis, call center statistics including, but not limited to, number of total incoming calls, total calls answered, number of calls answered within 20 seconds, number of calls abandoned, number of calls placed on hold in total duration of more than 5 minutes, number of call backs completed.

4.1.1.7 As directed by the National Defense Authorization Act (NDAA) of January 2008 (reference Section J, Attachment 9, p. 1,191 labeled 1,159), specialty consultations for Wounded Warriors will include identifying issues and coordinating with DoD, Veterans Affairs (VA), Department of Labor (DOL) and other federal agencies. The NDAA requires that DoD provide a secondary level of assistance to facilitate issues that are unresolved at the Service and other agency levels.

4.1.1.8 Specialty consultations for Wounded Warriors will follow DoD provided protocols to respond to all Wounded Warrior inquiries involving a report of deficiencies to assure that referrals are submitted within 1 hour of receipt to designated individual(s) within the respective Service Wounded Warrior program or VA to facilitate development of a Plan of Action within 96 hours of receipt of the call.

4.1.1.9 Consultations will involve frequent information exchange to institute this directed response to Wounded Warriors and their families, to include coordinating with military Services Wounded Warrior program

representatives, VA, and TRICARE to resolve Wounded Warrior issues (e.g., long delays in obtaining appointments, significant geographic distance from facilities, or complaints about the quality of services they receive).

4.1.1.10 The Contractor shall make outbound calls to specific groups within the served population. Follow-up calls will be made to military members and families in order to ensure that services delivered met the requirements, needs and expectations of the caller. Normally, approval to call back must be obtained from the caller on their original call for assistance. Additionally, in order to meet the changing needs of the military members, their families and the DoD – other specific call back services may be added.

4.1.1.11 The Contractor's technical infrastructure supports translation/interpretation. Contractor telephone integration shall include a process and capability to use interpreter/translators for telephone calls. Translation services will be offered on an immediate/on-demand basis to individuals calling the call center. Translation services will also be available for legal documents (leases, marriage licenses, adoptions, utility bills, legal documents, etc.) within 3 business days.

## **4.2 MOS WEBSITE INTERFACING**

### **4.2.1 MOS WEBSITE INTERFACING REQUIREMENTS**

4.2.1.1 The Contractor shall maintain the non-proprietary interface integrating its EAP service into the MOS website.

4.2.1.2 The Contractor shall provide a single entry point into the EAP services with a secure login capability as a user option. The Government requires access, but not ownership, to the vendor's EAP program. The Government shall maintain ownership of all data and content in front of the login, and all of the data behind the login contained within the vendor's case management system.

4.2.1.3 The MOS website shall comply with Section 508 of the U.S. Rehabilitation Act for website, voice and data services and content shall be available in both English and Spanish. At a minimum, compliance includes TDD/TTY (telecommunications device for the deaf); Interactive Voice Response Systems (IVRs)/Automated Attendants; voice mail systems; websites; and information systems.

4.2.1.4 The Contractor shall provide MOS EAP Services on a continuous basis. The Contractor shall provide these services by utilizing the following support methodology principles:

- Ensure physical and logical security for all hosted computer resources.
- Provide all necessary power and environmental controls to operate and maintain the equipment.
- Plan and implement 24/7 backup and recovery
- Implement and enforce DISA compliant security

## **4.3 MINIMUM REQUIREMENTS APPLICABLE TO BOTH MOS CALL CENTER AND ONLINE SERVICES**

4.3.1 The Contractor shall provide access to telephone and Internet services that meet the standards of Section 508, U.S. Rehabilitation Act.

4.3.2 The Contractor shall provide security to protect the confidentiality, integrity, and availability of data in accordance with (IAW) all applicable Federal Laws, regulations, policies, and industry standards in accordance with, appropriate access control, comprehensive intrusion detection, comprehensive virus protection, formal incident response procedures, vulnerability monitoring and mitigation, and periodic (at least annual) third party security assessments to ensure on-going effectiveness. (Reference Section J, Attachment 11)

4.3.3 Contractor shall ensure all data collection and storage systems provide for DoD level information and system security, protect the confidentiality, integrity, and availability of data in order of precedence with all applicable Federal Laws, DoD regulations and policies (reference Section J, Attachment 5), State laws, and industry



standards. Contractor shall ensure that all electronic data collection and storage systems are designed with access control, comprehensive intrusion detection, and comprehensive virus protection. Contractor shall develop and implement formal incident response procedures, vulnerability monitoring and mitigation.

4.3.4 The contractor's technical infrastructure and telecommunication capabilities support 24/7 call center operations to receive both CONUS and OCONUS calls.

4.3.5 The Contractor's technical infrastructure integrates the case management system with call center operations.

4.3.6 The Contractor's technical infrastructure integrates the call center data/analytics into reporting requirements.

#### **4.4 INFORMATION TECHNOLOGY (IT) AND INFORMATION ASSURANCE (IA) SERVICES**

4.4.1 Telephone integration shall include a process and a capability to use interpreter/translators for telephone calls in foreign languages (reference Section J, Attachment 10).

4.4.2 The Contractor shall provide expert-level IA support to establish, maintain, and enhance a robust, DISA/DoD compliant Information Assurance capability. The scope of this IA support shall include IA Project Management, Risk and Compliance Management, DIACAP Compliant Certification and Accreditation (C&A), Vulnerability Analysis, Assessment and Reporting, Security Engineering and Integration and Security Incident Response. The objective of this scoping is to:

- Provide the full capabilities to assessment risk of changes to the MOS system(s);
- Establish DIACAP compliant C&A packages on all required systems;
- Establish a robust vulnerability management capability that ensures standardized vulnerability testing, analysis, and reporting.
- Provide an Incident Response capability that follows required reporting requirements and quickly isolates, investigates, and remediates security incidents.

4.4.3 The Contractor shall meet all IA requirements IAW the most current DoD 8500 series of instructions (reference Section J, Attachment 16).

4.4.4 The Contractor shall deliver compliant, applicable IA controls as listed in DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP) (reference Section J, Attachment 18).

4.4.5 The Contractor shall provide personnel appropriately certified to support IA functions IAW DoDD 8570.01 (reference Section J, Attachment 17).

4.4.6 The Contractor shall meet all IA requirements as defined in the DISA Secure Technical Implementation Guidance (STIGs) except as authorized in writing by the DAA.

4.4.7 Disaster Recovery Planning (DRP) and Continuity of Operations (COOP) Support for EAP services. The Contractor shall provide support in planning for DRP/COOP. The Contractor shall provide presentations, reports, and diagrams which outlines the measures that will be required for DRP/COOP. The contractor shall audit the DRP and COOP process to ensure that it meets all applicable mandates and policies by MC&FP.

#### **4.5 CASE MANAGEMENT OBJECTIVE**

The Government requires a case management system capable of sharing data (import and export) in an Open Database Connectivity (ODBC) compliant format for use by the MOS Program and other QOL programs. Client information shall be maintained on the MOS Contractor's Case Management System. The case management system shall be capable of maintaining Client confidentiality/privacy while still providing access to the Client's previous requests for assistance, caller-identifying information, Client concerns, and support provided to the Client. The Case management system will support DoD reporting requirements.

#### **4.5.1 CASE MANAGEMENT SYSTEM MINIMUM REQUIREMENTS**

The Contractor shall identify and utilize a case management system that maintains Client confidentiality while still providing access to the Client's previous requests for assistance, caller-identifying information, Client concerns, and support services provided to the Client. The case management system should eliminate the need for the Client to repeat basic information on subsequent calls. Case management system functionality shall include the Client requests for the Contractor to assign a specific consultant to the case, whenever possible.

4.5.1.1 The Contractor shall provide case information, as identified by the Government, for input into the case management system. The information shall be sufficient to document services provided without violating client confidentiality

4.5.1.2 Contractor case management system shall be capable of automatically populating an on-line database of usage. Usage data may be updated to meet DoD information needs.

4.5.1.3 The Contractor's case management system is compliant with the Privacy Act.

4.5.1.4 The case management system tracks duty to warn cases.

4.5.1.5 The Contractor's case management system tracks emergent, urgent, and routine issues.

4.5.1.6 The case management system provides for web-enabled and access-leveled security.

4.5.1.7 The case management system provides a scheduler functionality to support follow-up tracking and the provision of additional services.

4.5.1.8 The case management system will segregate all DoD data from any data not belonging to the DoD. This will be a logical and physical segregation when at rest or in transition.

#### **4.6. MONTHLY REPORTS OBJECTIVE**

The Government requires detailed monthly MOS data and analysis of program utilization and quality for use in program monitoring and development. Details and accurate utilization and quality metrics will allow the Department and Military Services to redirect and refocus contract efforts and target marketing as required.

##### **4.6.1 MINIMUM REQUIREMENTS FOR MONTHLY REPORTS**

The Contractor shall deliver a Monthly Contracting Report and a Financial Disbursement Report. Submission shall be due monthly beginning on the 15th of the month following the first month of full performance and on the 15th of each month thereafter throughout the period of performance. Submissions of reports shall be in Windows Office (Word or Excel) format and sent via e-mail.

4.6.1.1 The Government will have ten days for review and acceptance/rejection of the monthly contracting and financial disbursement reports.

4.6.1.2 The Contractor shall capture and report all Service member and family member contacts by Military Service and installation, Service member or family member, to include Guard and Reserve, on a monthly basis. A complete list of current military installations can be found at the following link:

<http://www.militaryinstallations.dod.mil>

4.6.1.3 Required Data in Report – The Monthly Progress Report shall include, but will not be limited to:

4.6.1.4 Program Report. The monthly program report will include metrics on program utilization, call center and website traffic, counseling referrals and sessions provided, provider network capacity, customer satisfaction, and other data as required by the Government. A list of required data points is included in Section J, Attachment 21.

4.6.1.5 Financial Disbursement Report. The monthly financial report will include the total of invoices to date, the amount received in payments to date, the amount that has been invoiced but not paid and the funds remaining not invoiced. All information will be reported by CLIN/Sub-CLIN. A list of required data points for the financial report is included in Section J, Attachment 21.

4.6.1.6 In addition to the monthly reports, the Contractor will deliver ad-hoc reports to the program office as required.

4.6.1.7 The contractor will also submit an annual (fiscal year) report, including yearly totals of all reporting requirements listed above, not later than 60 days after the end of each period of performance.

4.6.1.8 The web-based/web-enabled case management system shall be able to produce on-call, on-demand reports that allow the Government to track usage, caseload, types of cases and other critical management and information needs as required by DoD. Reports will be available on-line and available as both Microsoft Word and Excel products.

#### **4.7 DISASTER CONTINUITY OF SERVICES OBJECTIVE**

The Government requires that client MOS services (1-800 Call Centers, Case Management System, etc.) are available 24/7 despite any natural or man-made disasters. In the event of a disaster, the MOS telephone number will serve as the primary information source for Clients.

##### **4.7.1 MINIMUM REQUIREMENTS FOR DISASTER CONTINUITY OF SERVICES**

In the event of a disaster, either natural or man-made, the contractor shall be able to maintain normal operations with no downtime or loss of data. The Contractor shall demonstrate capability for continuity of services to include redundancies for all MOS operations and systems.

4.7.1.1 Contractor shall develop and implement procedures to address organizational policy to prevent system shutdowns caused by disasters.

4.7.1.2 Contractor shall develop a test plan and execute it at least annually to ensure complete system shutdown is avoided and all MOS services remain available throughout any disaster or crisis situation. Based on the test results, the plan should be modified if required.

4.7.1.3 The Contractor shall provide a description of the company's current disaster continuity of services plan, which will include when it was last tested and type of testing performed.

4.7.1.4 The Contractor's disaster continuity of services procedures provide no down time and no loss of data.

#### **4.8 MILITARY UNIQUE REQUIREMENTS**

4.8.1 The Contractor shall utilize protocols and procedures established by the Government for Client usage of the call center. Protocols include, but are not limited to, warm hand-offs (i.e., 3-way telephone call with Client, MOS and referral organization) to TRICARE, the military health plan; SECO Program provider; referrals to non-medical counseling providers; and referrals to subcontractors that are providing services within the MOS suite of services. These protocols and procedures also include military community and family service agencies such as Army Community Services (ACS), the Navy's Fleet and Family, Marine Corps Community Services (MCCS), and Airman and Family Readiness. The procedures for warm hand-off will ensure that client does not have to repeat their story or issue when the third party agency is engaged in the conversation. Similar protocols will be utilized to connect interested Clients to the various injured support programs as required and as established by the Government.

4.8.2 The Contractor must establish and maintain a customer-service atmosphere of respect and concern for every Service member or family member, regardless of grade/rank, ethnicity, education, sophistication or problem.

4.8.3 The Contractor shall develop and conduct initial and ongoing training for call center staff to familiarize them with military customs, traditions, environment, benefits, and military programs. Call center staff shall be familiar with evolving issues that affect military members and their families.

## **TASK 2 NON-MEDICAL COUNSELING**

### **5.0 NON-MEDICAL COUNSELING OBJECTIVE**

To provide private, confidential non-medical counseling, which includes problem solving, financial, health and wellness, to Service members and their families. The counseling support is intended to augment, not replace, existing military/civilian support services, and Service or Component funded staff positions/programs. The counseling programs should ensure support is provided when and where it is needed. The counseling programs will address the stressors of military life and will assist Service members and their families in dealing with deployments, effects of war, relationships, crisis intervention, stress management, family issues, communication, family separations, reunions and reintegration due to deployment, financial concerns and healthy living. The non-medical counseling services are an integral part of military and family support programs that are targeted to ensure personal and family issues do not detract from operational readiness; to strengthen individuals by assisting them in the problem-solving process and to increase individual and family member competencies and confidence. These programs are delivered and maintained IAW standard and professional EAP including additional aspects specifically pertaining to the MOS non-medical counseling programs. Non-medical counseling programs are intended to be solution-focused, short-term for defined problem areas amenable to brief intervention. Services are usually delivered in the traditional manner of fifty minute sessions in an office setting, face-to-face (CONUS only), to individuals, couples, families, and groups, and telephonically or over the Internet to eligible individuals worldwide. Eligible participants may receive up to twelve non-medical counseling sessions per person per issue at no cost to the Client.

#### **5.0.1 SCOPE**

Non-medical counseling program services are available to all Service members and their families as specified in Section 1.2 of this PWS.

For problem-solving counseling support, scope is defined as follows:

- Appropriate issues for non-medical, short-term, solution-focused, problem-solving counseling services include, but are not limited to, subclinical (v-code) issues such as:
  - Relationship issues, parenting skills, communication;
  - Relocation, academic or occupational problems;
  - Anger management, grief, stress, adjustment, deployment, reintegration, separation;
  - Phase of life, decision-making, life skills, coping skills and interpersonal skills;
- **Inappropriate issues** for non-medical, short-term, solution-focused, problem-solving counseling services include, but are not limited to:
  - Post Traumatic Stress Disorder (PTSD), Traumatic Brain Injury (TBI), and any mental disorder identified in the Diagnostic and Statistical Manual of Mental Disorders, Latest Edition, are NOT authorized for non-medical counseling support, and will be referred (via a warm handoff) to the appropriate MTF, TRICARE or community mental health provider;
  - Chronic or multiple issues stemming from underlying conditions that are more ingrained or severe, including substance-related disorders;
  - Active suicidal/homicidal thoughts or intent or other threats of harm to self or others;

- **Inappropriate situations include:**

- If Client is working with a mental health professional or prescriber of psychoactive medication or has a history of recurring in-patient mental health treatment;
- If Client has an open case with Family Advocacy Program (reference Section J, Attachment 15), Victim Advocate, Sexual Assault Response Coordinator or child protective services and this includes if a Mandated report or Duty-to-Warn report is indicated;
- If Client is requesting a formal evaluation, assessment or treatment regarding fitness for duty, return to work recommendation, medical leave documentation/ recommendation and/or court-ordered.

5.0.1.1 Face-to-face counseling services are provided within the civilian community.

5.0.1.2 Reserved.

5.0.1.3 Non-medical counseling providers may not self-refer for clinical mental health therapy. At the time a Client is determined to need clinical mental health counseling, the MOS provider is to notify the Prime Contractor and provide a warm handoff or referral directly to TRICARE, the MTF or community resources for determination of who will provide clinical support. The MOS provider will not imply or engage self-promotion to secure clinical referrals for MOS Clients. It is imperative appropriate support services be engaged when working with MOS Clients.

5.0.1.4 MOS non-medical counseling services focus on a specific issue or concern and include developing strategies and solutions building on the Client's strengths, accessing support systems, and utilizing community resources.

5.0.1.5 The Contractor is responsible for ensuring MOS staff and non-medical counseling providers adhere to the scope of practice for MOS Non-Medical Counseling Programs.

## **5.0.2 CONFIDENTIALITY**

5.0.2.1 All employees, contractors, and subcontractors who will have access to Client information will be advised of the confidential nature of the information, that the records are subject to the requirements of the Privacy Act of 1974, and that unauthorized disclosures of Client information may result in the imposition of possible criminal penalties.

5.0.2.2 The Contractor shall establish and maintain a record keeping system that is designed to protect the Service member or family members' privacy and confidentiality, as appropriate and required for specific services. Written records of the content of the counseling session must be maintained by MOS staff or network provider who is providing support. Although this counseling is private and confidential, the contractor must keep utilization records for quality assurance which document confidential and private services have been provided to service members and their families. The MOS staff or network provider must explain to the Service member or family member that the personal identification information will be held in strictest confidence by the Contractor and not shared with the military command with exception of Section 5.0.4. in this PWS.

5.0.2.3 When the military chain of command requests information concerning a Service member, they are reminded of the confidential nature of the service. If the chain of command wishes to send a Service member for counseling to a MOS staff or network provider and have the MOS staff or network provider report back to the commander, they are informed that this is not possible due to the confidential nature of the program; however, they are informed that if they sent a Service member to see a MOS staff or network provider they may follow up with the service member to ensure that they followed through.

### **5.0.3 INFORMED CONSENT**

5.0.3.1 IAW DoD Instruction No. 6490.06, Counseling Services for DoD Military, Guard and Reserve Certain Affiliated Personnel and Their Family Members (reference Section J, Attachment 20), MOS staff and network providers shall provide informed consent to the individual and/or family member during the initial contact covering information about their role as MOS staff or network provider, a description of what non-medical counseling can cover, the short-term solution focused approach, the scope of care, and the ability to make appropriate referrals as needed.

5.0.3.2 Informed consent must cover the MOS staff and network provider's mandated reporting requirements for domestic abuse, sexual assault, duty to warn and other legal obligations. At a minimum, the following confidentiality statement shall be provided to all eligible individuals seeking counseling services:

- "Information you provide to me or other counselors will be kept confidential, except to meet legal obligations or to prevent harm to self or others. Legal obligations include requirements of law and DoD or military regulations. Harm to self or others include suicidal thoughts or intent, a desire to harm oneself, domestic violence, child abuse or neglect, violence against any person, and any present or future illegal activity. For Personnel Reliability Program (PRP) certified members, reporting any concerns related to reliability is also required."

### **5.0.4 IMMINENT RISK/DUTY TO WARN/MANDATED REPORT**

5.0.4.1 The Contractor shall develop and maintain established processes and procedures for its obligations as it applies to Duty to Warn and Mandated Report issues in the event a Client reveals such information.

5.0.4.2 The Contractor shall implement, document, and maintain Duty to Warn procedures, IAW DoD/Military Branch of Service and Component regulations and established protocols, to address events wherein a Service or family member reveals a threat to self or others. Mandated reports including, but not limited to, child abuse/neglect, domestic abuse/violence, sexual assault, illegal activity, PRP report, shall be engaged IAW established military, state, and federal requirements and regulations and shall be included in the Duty to Warn monthly report. Notifications of Duty to Warn and Mandated Report incidents are reported to the appropriate authorities and Contractor chain of command immediately.

5.0.4.3 Duty to Warn/Mandated Report monthly report logs shall be compiled and sent to the Government MOS Program Office and be reported as mandated, to the respective, federal and state authorities. This report log shall include, at a minimum: date of event, installation name, state, name of the unit, status (new vs. recurring), category (domestic violence, child abuse, harm to self/others), branch/component of service, summary of events, action taken and any other pertinent information. This report log shall not include any personally identifiable information.

### **5.0.5 DOCUMENTATION**

5.0.5.1 Formal documentation of all non-medical counseling services pertaining to all MOS Clients is required.

5.0.5.2 The Contractor shall retain documentation as required on all non-medical counseling cases. Formal counseling case records including personally identifiable information will be maintained by the Contractor. Case records will be provided for quality assurance review upon request of the Government MOS Program Office.

### **5.0.6 WARM TRANSFER/REFERRAL PROCESS**

5.0.6.1 If the Client requests non-medical counseling during the initial contact, the Contractor shall ascertain if the Client's issues are in scope for services and, if so, directly handoff the Client to a non-medical counselor immediately for telephonic, web-based, or face-to-face counseling. If the Client's issue is determined to be out of scope for services, a warm handoff is required for Emergency situations and preferred for Urgent and Non-Urgent calls.

5.0.6.2 The procedures for a warm handoff will ensure that Client does not have to repeat their story or issue when the third party agency is engaged in the conversation. During the warm handoff overlap, the Contractor staff or network provider shall, at a minimum, maintain a no-hold telephonic connection and convey pertinent information citing the Client issues are out of scope, or in need of specialized services not provided by MOS, and ensure a verbal connection is secured prior to exiting the warm handoff telephone connection. No identifying information shall be provided without the expressed consent of the Client for a referral and no identifying information provided when implementing a warm handoff.

5.0.6.3 The Contractor shall attempt to satisfy Client preferences regarding age, gender, culture, and language when providing referrals for non-medical counseling.

5.0.6.4 The Contractor shall utilize protocols and procedures established by the Government MOS Program Office, and include, but are not limited to, warm handoffs (i.e., 3-way telephone call with Client, MOS and referral organization) to TRICARE, the military health plan; referrals to the SECO Program provider; referrals to non-medical counseling providers; referrals to network providers; and referrals to subcontractors that are providing services within the MOS suite of services. These protocols and procedures also include military community and family service agencies such as Army Community Services (ACS), the Navy's Fleet and Family, Marine Corps Community Services (MCCS), and Airman and Family Readiness. Similar protocols will be utilized, as established by the Government, to connect interested Clients to the various injured support programs as required.

## **5.0.7 FOLLOW-UP**

With the Client's approval, the Contractor shall make outbound calls to all non-medical counseling Clients. Follow-up calls will be made to military members and families in order to ensure that services delivered met the requirements, needs and expectations of the caller. Normally, approval to call back must be obtained from the caller on their original call for assistance. Additionally, in order to meet the changing needs of the military members, their families and DoD, other specific call back services may be added, at the direction of the Government.

## **5.0.8 NOTIFICATION OF ADVERSE INCIDENT**

The Contractor shall develop and maintain a process for immediate notification (within 24 hours) to the Government MOS Program Office of any situation or incident that could potentially generate negative media or other attention on the program.

## **5.0.9 NON-MEDICAL COUNSELING PROVIDER REQUIREMENTS**

### **5.0.9.1 CREDENTIALING**

All network providers and supervisors must have submitted required documentation and have undergone credentials review/verification by the contractor of all items in this section prior to performing under this contract.

5.0.9.1.1 The Contractor shall not utilize a network provider for non-medical counseling, at any location at any time during the performance of this contract, until a Criminal History Background Check and Fingerprint Check have been initiated (submitted to appropriate agency completing the check). Contractor personnel/providers who have previously received an acceptable Criminal History Background Check and Fingerprint Check shall provide proof to the prime Contractor prior to performing under this contract. The level of Criminal History Background Check and Fingerprint Check shall be at a minimum the same level described in DoD Instruction No. 1402.5 (reference Section J, Attachment 19) for all non-medical counselors/providers. Criminal History Background Checks and Fingerprint Checks must be completed within 90 days of initiation. Parental approval, documented in writing, is required for all Participants under the age of 18 receiving non-medical counseling services. Duty to Warn or Mandated report situations do not require parental/guardian approval in order to report to authorities.

5.0.9.1.2 Non-medical counseling providers must adhere to commercial and professional standards of practice set forth by federal, state, and local laws, as well as relevant DoD/Military Branch of Service and Component policies. All network providers must be licensed, certified, properly credentialed to perform this requirement and be

compliant with the commercial industry accepted standards for the performance of EAP programs and non-medical counseling.

5.0.9.1.3 The Contractor shall annually certify and be able to demonstrate (at any time) to the Government MOS Program Office or the Contracting Officer (CO), in writing, that the non-medical counseling providers and supervisors licensure, credentials, required experience and background checks are current and proper for performance under this contract. This certification shall verify that the network provider has not experienced any terminations of performance under any other government contract or any license suspensions or any investigations. Network providers, who have experienced any of the aforementioned actions, will not perform services under this contract. The Contractor shall certify, upon award and the exercise of each option period, that all non-medical counseling providers and supervisors are properly licensed or certified, comply with the appropriate background check requirements, and possess all other qualifications as indicated in the PWS prior to beginning work with a MOS Client. The Contractor shall maintain all non-medical counseling provider /supervisor certifications and background check documentation for the life of this contract, and make them available for Government review at any time during performance.

## 5.0.9.2 TRAINING

The Contractor shall develop and maintain a training program and methodology to ensure MOS staff and network providers are current on military services specific issues and understand military terminology and the issues facing the Client. This training program shall include, but is not limited to:

- Orientation explaining the parameters of the program, the prohibition on providing clinical mental health therapy, the scope of support services and programs, and the referral process as well as Restricted Reporting, Mandated Reporting and Duty to Warn protocols. This must include FAP procedures and protocols as well as other service entities with whom they may come in contact regarding a Restricted Reporting referral, Mandated Report or a Duty to Warn. Processes and procedures to support the warm handoff of Clients to other providers and community resources shall also be addressed;
- Scope of Practice;
- Training on military culture and sensitivity;
- Standardized training and guidance on each service component to include: Army, Navy, Air Force, Marine Corps, Army National Guard, Army Reserve, Air National Guard, Air Force Reserve, Marine Corp Reserve, and Naval Reserve;
- Training on required documents such as Intake Assessment, Progress Notes and Case Closure including submission deadlines and methodology;
- Guidance for MOS network providers in the event of a disaster;
- Training specifically regarding deployment and reintegration;
- Training on evidence-based care for assessment, management and intervention of suicide-related behavior;
- Post-suicide survivor training;
- Mandated and Duty to Warn process or reporting.

5.0.9.2.1 The Contractor shall design and implement a method for regularly updating personnel on current/emerging issues pertaining to military life. MOS staff and network providers shall be familiar with evolving issues that affect military members and their families.

5.0.9.2.2 All required training, including subject matter tests, must be completed successfully **prior to** being referred or working with a MOS Client. Training must be renewed on an annual basis.

5.0.9.2.3 The Contractor shall annually certify and be able to demonstrate (at any time) to Government MOS Program Office or the CO, in writing, that the MOS staff and network providers and supervisors have comprehensive/current knowledge of the scope of practice, overall military culture, issues affecting military families, and all requirements of this contract.



### **5.0.9.3 ADVOCACY KNOWLEDGE, SKILLS AND ABILITIES**

All non-medical counseling providers shall possess advocacy knowledge, skills, and abilities including, but not limited to:

- Understanding, sensitivity, and empathy for Service members and their families. Ability to develop trusting helping relationships. Ability to work effectively with individuals and families from diverse racial, ethnic, and socioeconomic backgrounds;
- Ability to intervene in crisis situations, using sound professional judgment, ethical practice, and common sense. Network providers must work independently to develop, implement, and evaluate safety and intervention plans to meet individual and family needs. Contractor must agree to operate within established guidelines of the military services family support and quality of life programs;
- Ability to work cooperatively with military and civilian medical, social service, law enforcement, financial support organizations and legal personnel on behalf of service members and their families;
- MOS staff and network providers should be computer literate. It is preferable that they possess the basic computer skills to enable them to enter data in required management reports and utilize information systems to prepare required reports and information;
- Sound professional judgment and the highest ethical standards in executing their responsibilities. MOS staff and network providers shall have strong skills in written and verbal communication, and assessment.

5.0.9.3.1 The network providers shall establish a schedule that allows for regular contact with the Contractor during office hours yet is flexible enough to be responsive to family needs after hours. Network providers' hours will be flexible to meet the needs of the families which may include evenings and weekends as needed for meeting with families.

5.0.9.3.2 MOS staff and network providers must be knowledgeable of the resources available through the MOS website ([www.MilitaryOneSource.com](http://www.MilitaryOneSource.com)) to access additional capabilities through MOS when circumstances warrant.

## **5.1 REQUIREMENTS FOR ALL TYPES OF NON-MEDICAL COUNSELING**

The Contractor shall provide access to a national network that provides non-medical counseling to Clients. The Contractor shall ensure that all personnel maintain the highest degree of sensitivity, compassion, and respect for service members and their families.

5.1.1 The Contractor shall remain free of any political bias and shall ensure consistency of service regardless of installation, location, or any other factor.

5.1.2 The Contractor shall capture selective Client contact and demographic information, to include ensuring that Clients meet Military eligibility criteria, while ensuring Client confidentiality, in a database/s and provide monthly reports detailing non-medical counseling services, that includes at a minimum, the duty status and rank of counseling participants, type of counseling (i.e., marital, grief & loss, parenting, communications, financial, etc), number of sessions, distance of network provider from residence of participant and other data points as required by the Government.

5.1.3 The Contractor shall maintain procedures for responding to Emergency, Urgent, and Non-Urgent calls. These procedures shall include an immediate response for Emergency situations, access to non-medical counseling within one business day for Urgent Clients, and access to non-medical counseling within three business days for Non-Urgent calls. A warm handoff is required for Emergency situations and preferred for Urgent and Non-Urgent calls.

5.1.4 All program aspects of the MOS non-medical counseling programs must be approved by the Government MOS Program Office. No modifications, processes, policies or procedures can be implemented without written approval from the Government MOS Program Office.

5.1.5 The Contractor will adhere to written protocols for each type of service delivery.

5.1.6 If a region is confirmed to require additional network provider support, the Contractor will initiate recruitment of additional network providers, as is possible. The Contractor will report to the Government MOS Program Office monthly regarding network provider coverage.

5.1.7 The Contractor shall develop and implement an approach and processes to manage network providers, ensuring timeliness and efficiency and avoiding disruption or degradation of services. This approach shall account for the complexities of network providers providing field services and shall also account for short notice or immediate requirements that require expedient response. The Contractor's network shall assure access to face-to-face counseling is within fifteen miles or thirty minutes of the Client. Problem-solving and financial counseling services must be provided on a face-to-face basis when requested (CONUS only).

5.1.8 The contractor shall comply with the DoD Directives and Instructions, to include all future updates, referenced in Section J, Attachment 11.

5.1.9 MOS staff and network providers are also not authorized to speak to the media/press regarding MOS or their work with MOS Clients without specific written approval from the Government MOS Program Office. MOS staff and network providers shall not engage in political discussions with Clients concerning military policy as they must remain focused on providing support. MOS staff and network providers will not represent the Government at any federal, state, or military meeting or event.

5.1.10 All MOS staff and network providers performing this requirement must be a U.S. citizen, and must speak English.

5.1.11 MOS staff and network providers shall also be available by telephone, enabling counseling participants to schedule an appointment for MOS services.

5.1.12 MOS staff and network providers may not transport any MOS-connected Client in any vehicle.

5.1.13 MOS staff and network providers will verify eligibility for services, which may include requesting to view a military identification card.

## **5.2 OBJECTIVE FOR PROBLEM SOLVING COUNSELING ONLY**

Provide private and confidential non-medical, short-term, solution-focused counseling services for circumstances amenable to non-medical, brief intervention. The counseling approach used is psycho-educational, to empower participants to learn to anticipate and resolve challenges associated with the military lifestyle. This non-medical support is aimed at preventing the development or exacerbation of mental health conditions that may detract from military and family readiness. This program does not provide clinical mental health therapy.

### **5.2.1 MINIMUM REQUIREMENTS FOR PROBLEM SOLVING COUNSELING ONLY**

Problem-Solving Counseling providers shall have at least a Masters degree from an accredited graduate program in a mental health related field such as social work, psychology, marriage/family therapy, or counseling; a valid unrestricted counseling license/certification from a State, the District of Columbia, a U.S. Commonwealth, or a U.S. Territory that grants authority to provide counseling services as an independent practitioner in their respective fields; and demonstrated counseling competence preceding their employment with the MOS program. The Contractor's national network shall assure access to face-to-face counseling for Clients within established parameters for delivery of service.

5.2.1.1 In addition to meeting the above requirements, the non-medical network provider supervisors must have a minimum of two years full-time counseling experience post-licensure; documented counseling supervision, oversight, and management experience; and demonstrated current counseling competence through at least periodic, direct service counseling experience during the two years preceding hire.

### **5.3 OBJECTIVE FOR FINANCIAL COUNSELING ONLY**

Service members are responsible for their personal finances. Throughout a military career, service members and their families may need additional support and assistance with financial stability, money management, anticipating financial impacts due to deployments, and raising a financially stable family. Accredited and certified network providers trained in financial matters shall provide personal and family financial counseling, planning, education, awareness information services, appropriate referrals, and assistance applicable to military families. Counseling services may be provided individually, couples, families, and in a group training environment.

The goal is to assist service members and their families with personal financial readiness, money management, financial counseling, and financial planning to include appropriate guidance regarding the Service member's Civil Relief Act, Public Law 110-289 Housing and Economic Recovery Act of 2008 as well as other pertinent laws and policies. The majority of service members and their families will require financial counseling to assist with establishing a basic level of financial literacy and good financial behavior and habits, as well as more sophisticated financial planning to assist with more advanced financial needs such as investing, estate planning, tax planning, education planning, and other financial matters.

#### **5.3.1 REQUIREMENTS FOR FINANCIAL COUNSELING ONLY**

MOS financial staff and network providers shall have a minimum of a Bachelor's degree and shall maintain a national certification as an Accredited Financial Counselor (AFC), Certified Financial Planner (CFP), Chartered Financial Consultant (ChFC), or a national certification with the National Foundation for Credit Counseling (NFCC).

5.3.1.1 Contractor shall follow Government guidelines regarding employment and conflicts of interest. Financial network providers shall provide service delivery that meets the standards in DoD Instruction No. 1342.27, "Personal Financial Management for Service Members," (reference Section J, Attachment 13) and assist service members and their families with personal financial readiness.

5.3.1.2 This type of counseling is provided telephonically or face-to-face generally using a planned meeting approach.

5.3.1.3 In cases of extreme financial hardship, threat of deprivation, or other similar circumstances, financial network providers ensure that service members and their families are referred to the appropriate military resources such as Relief Societies, installation banks/credit unions, Chaplains, other state, federal, local and veterans' organizations, and other resources as applicable.

5.3.1.4 MOS financial staff and network providers shall provide individualized money management, financial counseling, financial planning, and referral services when applicable, to service members and their families. However, MOS financial staff and network providers will never give specific financial investment advice in specific investment funds/opportunities. The following list is not exhaustive and meant only to provide examples of potential activities MOS financial staff and network providers may conduct:

- Complex financial planning and investment issues and opportunities.
- Advice and assistance in such areas as prioritizing and understanding differences between needs and wants.
- Identifying immediate and long range measures to increase income, reduce household expenditures, avoid additional financial burdens; developing improved financial record-keeping.
- Creating a personal budget/financial plan to reduce, eliminate, and avoid debt and to achieve solvency and stability.
- Fostering recognition of the legal and military implications of indebtedness and recommending legal assistance if warranted.
- Teaching service members and their family's money management techniques to encourage them to live within their means.
- Identity theft: teaching service members and families how to detect, deter, and avoid identity theft.

- Credit management: understanding credit, finance charges, interest rates and the implications of only paying the minimum amount each month.
- Credit: educating military families on the importance of maintaining excellent credit histories and ratings. Teaching service members and their families how to establish, monitor, and protect their credit. Poor credit may cause service members to lose their security clearances.
- Housing: Purchasing a home, preventing foreclosure, loan modifications, refinancing, etc.
- Car Buying: teaching service members to make informed decisions and to be aware of associated costs such as insurance, maintenance, fuel costs, etc.
- Investing/retirement: PFCs reach out to young service members to get them enrolled in the Thrift Savings Plan (TSP). PFCs shall be equipped to explain the benefits of investing and reducing tax liabilities.
- Assistance with tax planning.
- Managing special duty pay.
- Routine Savings: teaching service members and their families how to save for emergencies, unanticipated contingencies, and both short and long-term goals.
- Decision making regarding appropriate type and amount of insurance to carry to include understanding the value of Service member's Group Life Insurance.
- Military-specific financial programs and benefits: teaching service members and their families about the value and benefits of participating in the Thrift Savings Plan, the Savings Deposit Program, and Morale, Welfare, and Recreational programs.

### **5.3.2 MINIMUM REQUIREMENTS FOR TAX FILING SERVICES**

Contactor shall provide tax filing support that allows Service members access to free tax filing services for Federal and multiple state returns via the MOS website. MOS Clients will be able to link directly to the tax filing service.

5.3.2.1 Contractor is required to offer telephonic tax assistance counseling to assist Clients with their tax filing questions.

5.3.2.2 Contractor will develop a list of most frequently asked/answered tax questions and post these questions to the MOS web site.

5.3.2.3 Contractor shall provide contact information to MOS clients for the local military installation tax service support.

5.3.2.4 Contractor shall establish quality control procedures for tax service support specific to the Military population unique tax issues.

5.3.2.5 Contractor shall provide a monthly status on usage, by month and cumulative, for state and Federal filings and report this data IAW Monthly Status and Progress Report requirements under the Deliverables table (reference Section F.4 and Section J, Attachment 21). The contractor shall obtain Government approval of the tax assistance support plan prior to implementation.

5.3.2.6 Training for all counseling staff shall include ongoing familiarization with issues relevant to members of the military community.

5.3.2.7 Contractor shall encourage Clients to maximize the use of tax refunds, i.e., savings, paying down debt.

### **5.4 OBJECTIVE FOR HEALTH AND WELLNESS ONLY**

Contractor shall provide information and guidance on achieving and maintaining physical fitness and establishing healthy habits. Health and Wellness coaching is designed to educate and assist service members and their families in improving their health.

#### **5.4.1. MINIMUM REQUIREMENTS FOR HEATH AND WELLNESS ONLY**

MOS staff providing health and wellness coaching shall have at least a Bachelor's degree from an accredited college program in a mental health-related field such as social work and psychology and demonstrated current coaching competence preceding their employment with the MOS program.

5.4.1.1 Coaching sessions are provided telephonically and/or web-based, generally using a planned meeting approach.

5.4.1.2 The program will include a lifestyle health assessment, personal goal setting and coaching, and non-monetary incentives to assist service members and families attain and maintain their health and wellness goals.

5.4.1.3 Sessions may be conducted pertaining, but not limited, to:

- Fitness and exercise
- Diet and eating habits
- Health
- Goal setting
- Outreach and engagement
- Life Health Assessment

### **TASK 3 OTHER MOS PROGRAMS**

#### **6.0 OTHER MOS PROGRAMS**

The Government's objective for each of the program support centers are defined below:

#### **6.1 SECO OBJECTIVE**

The Government requires the Contractor to participate in transitioning the SECO Program to the vendor that has been selected to provide these specific services under a separate contract. The Contractor shall cooperate and coordinate with the new vendor to ensure transition occurs seamlessly. During the transition process, the Contractor is required to continue providing the SECO operational support described below until the transition is complete. This operational support may phase out slowly over time as the transition to the new vendor progresses. Once the transition to the new vendor has been completed, the Call Center triage consultants will answer calls for the SECO Program, which includes the SECO Career Center. If a caller is determined to need education or career information or counseling, or information regarding the My Career Advancement Account (MyCAA) Program or Military Spouse Employment Partnership (MSEP) Program, the call will be transferred to a SECO Career Center counselor, via warm hand-off, during SECO Career Center regular operating hours.

The Government's objective for the SECO Program is to have a service dedicated to providing the 1.2 million military spouses of Service members with education and portable career development counseling and information via telephone and/or from the internet in the following four pillars of the program:

- **Career Exploration/Discovery** offers spouses assistance with identifying career interests, aptitudes, and goals, high growth occupations, salaries, geographic factors, and self assessments, etc.
- **Career Education and Training** offers assistance with identifying career education/training requirements and service providers, state occupational licensing/credentials requirements, and financial aid resources.
  - This includes assistance with the MyCAA program:
    - Eligibility for MyCAA financial assistance is restricted to spouses of active duty Soldiers, who are serving on Title 10 orders, and in the pay grades of E1-E5, W1-W2, and O1- O2.

- MyCAA can pay up to \$4,000 for requirements leading to an Associate's degree, license, or credential in a portable career.
- MyCAA funds must be used within three years of the start date of the first class.
- Spouses ineligible for MyCAA are provided information on other sources of financial aid, to include federal, state, and private sources. MyCAA information can be found on the MyCAA web portal at: <https://aiportal.acc.af.mil/mycaa/>
- **Career Readiness** offers spouses assistance with resume preparation, interview techniques, employment ready self assessments for child care, transportation, virtual work, etc.
- **Career Connections** offers spouses seeking employment assistance with identification of employers eager to hire military spouses and federal employment opportunities, and includes referrals to the DoD Military Spouse Employment Partnership (MSEP) program, USAjobs.gov and installation Family Support Center staff for linking to local employment opportunities.

Provide Career Exploration/Discovery education, career and employment counseling services for military spouses world-wide to serve the approximately 1.2 million spouses of Service members, to assist spouses in learning about the Military Spouse Career Advancement Account Program and provide information regarding eligibility, education and employment questions. The service shall also be a source of advice for military spouses regarding federal, state and local career licenses and certifications requirements in portable career fields of education, health services, information technology, financial services, construction and any other portable careers suitable for military spouses.

#### 6.1.1 MINIMUM REQUIREMENTS OF SECO

SECO Counselors will offer all military spouses of service members world-wide personalized assistance with a self-assessment/analysis of career skills and interests to explore portable careers; assistance with identification of training/ education and licenses/credentials requirements necessary to achieve a portable career, assistance with assessment of readiness to enter the workforce, and referrals to employment opportunities such as the Military Spouse Employment Partnership and USAjobs.gov. Services will include, but are not limited to:

- Assistance with assessing personal skills, interests and aptitudes and other career self-assessments
- Assistance with identifying, planning, and evaluating educational and training goals
- One-on-one specialty education and career development consultations via the telephone
- Assist in planning academic life and career goals
- Provide information regarding specializations and levels of training required by educational and career choices
- Provide information regarding career credentialing and licensing requirements across state boundaries
- Identify appropriate educational resources and costs to include campus and on-line resources
- Identify projected salary/compensation by full range of careers
- Follow up with spouses entering educational/training programs funded
- Link to the US Departments of Labor and Commerce, US Department of Education, State resources and other education and career employment programs/web sites as directed by DoD
- Develop data banks of education/training institutions, education financial costs, portable career requirements, salary projections and credential/license requirements and other aspects of education and career development.
- Assist with employment readiness skills needed to obtain a job (i.e., resume writing, interview skills, requirements for child care/transportation, virtual/part-time employment, etc.)
- Identification of federal, state, and private sources of funding for education/training programs to include: degrees, courses, licenses and certifications

Additionally, military spouses of E1-E5, W1-W2 and O1-O2 are eligible for financial assistance funded by DoD through Military Spouse Career Advancement Accounts (MyCAA). This assistance includes, but is not limited to: individual military spouse MyCAA account creation, assistance in determining spouse eligibility,

review/approve education and training plans, financial assistance documents, and vetting schools for participation in the MyCAA program.

6.1.1.1 The SECO Program Manager must have a Master's Degree in Education/Guidance Counseling with a minimum of five years experience as a professional Education Counselor.

6.1.1.2 The Spouse Career Counselors must possess, at minimum, a Bachelor's degree with at least 2 years experience in education and career counseling.

6.1.1.3 The SECO program will be staffed from seven am until ten pm (7am-10pm) eastern time Monday through Friday and from ten am until five pm (10am-5pm) eastern time on Saturday.

6.1.1.4 Contractor will establish and maintain a summarized record of contact with each Client (i.e., school officials, spouses, etc.) contacted via email or telephone call. Client may call back and shall not have to repeat previously provided information or status of education/career direction.

6.1.1.5 Contractor will focus educational and career counseling on portable careers and occupations as identified by DoD to include education/training requirements, opportunities for on-line/distance education/training, school admission requirements, salary potential and projected future growth of career field nationally, portability of career choices, state, local and federal occupational licensing and credentialing requirements and associated costs, and assistance with resume preparation using the LinkedIn resume template.

6.1.1.6 Counselors shall provide spouses guidance on the use of the internet to obtain employment; assist with professional credentialing and licensing requirements; develop interview skills and provide information on occupations and salaries; and assistance with career planning and transitions.

6.1.1.7 Contractor will provide spouses with information on the SECO service. Staff will collaborate with the DoD program managers of the SECO initiative in providing services to eligible military spouses. Initial focus shall be on, but not limited to, the high growth portable career fields such as:

- Health Services
- Information Technology
- Education Services
- Financial Services
- Construction Trades (plumber, electrician, carpenter, etc)
- Human Resources
- Business Management
- Hospitality Management
- Homeland Security

6.1.1.8 Contractor, in concert with DoD, will develop protocols and scripts for use in communicating with military spouses regarding the full range of SECO services to include career exploration, education and training, licenses and credentials, career readiness and referral to employment sources such as MSEP, USAjobs.gov, and job fairs.

6.1.1.9 Contractor will work with Government SECO program managers to develop weekly reporting requirements for the SECO program. This requirement will include but is not limited to assistance to number of spouses by each of the four SECO pillars, number of phone calls, oldest call in queue to be returned, average handling time of calls, Spouse Career Center web site usage, etc.

6.1.1.10 The Contractor shall maintain advising records/notes for each military spouse SECO program participant via a secure intranet application that allows SECO staff to enter and view notes related to spouse SECO support.

## **6.2 JFSAP OBJECTIVE**

JFSAP teams serve Service members and families from all Components who are geographically isolated from

installation support and collaborate with existing family support resources to augment their activities and fill gaps where they exist. Services are delivered in local communities through collaborative partnerships with federal, state, and local entities, enhancing community capacity to serve military families.

#### **6.2.1 MINIMUM REQUIREMENTS OF JFSAP**

Contractor shall provide MOS Consultants to all states and territories to support increased outreach and coordination to geographically isolated service members and their families as military operations dictate. These MOS Consultants act as liaisons between MOS, DoD, the State Joint Force Headquarters, and National Guard Joint Force Headquarters Command. The JFSAP staff will travel throughout the state, as appropriate, to meet with families and unit family support staff to assess needs, form relationships with community resources, and provide or refer to services via a warm "hand-off." Also, reference Section J, Attachment 12 for Position Descriptions for JFSAP MOS consultants.

6.2.1.1 JFSAP staff will partner with and augment activities of Service Family Centers, Guard and Reserve programs (including Inter-Service Family Assistance Committees (ISFACs), unit family support staff officers, and other programs and services to build coalitions and connect Federal, state, and local resources and non-profit organizations to Active Duty, Guard and Reserve families.

6.2.1.2 JFSAP MOS Staff shall provide the following services and resources:

- Identify family needs;
- Catalogue existing family programs and supportive resources; determine how well those efforts are meeting family needs;
- Identify problems and/or gaps in service/resources;
- Determine methods to fill the gaps and enhance existing support systems' efforts; and
- Plan and implement a comprehensive, integrated, mobile service delivery system.
- On-demand support for Yellow Ribbon Reintegration Program (YRRP) and other deployment events

### **TASK 4 PROGRAM OVERSIGHT**

#### **7.0 PROGRAM OVERSIGHT OBJECTIVE**

To establish a dedicated program management team of key personnel to assure the consistent delivery of high quality services to the Clients.

#### **7.1 MINIMUM REQUIREMENTS FOR PROGRAM MANAGEMENT**

The Contractor Program Management Team shall include, at a minimum:

- Program director with the authority to speak and act on behalf of the contractor with DoD and to work directly with the COR.
- A deputy program director to assist the program director in managing this contract and able to act in the absence of the program director.
- A Lead for call center operations.
- A counseling supervisor who will be responsible for all of the counseling programs including non-medical, financial as well as coaching.
- A quality assurance program manager, who will ensure that all of the quality assurance programs, metrics (reference Section J, Attachment 7), reports and data are gathered, managed and reported within contract standards.
- A Lead who will be responsible for the management of all the various specialty programs and centers
- A Technical Lead responsible for all information technologies and communication resources deployed under and for this PWS.
- An Information Security Manager responsible for the implementation and management of security and availability of the outline platforms, equipment and software. This position will be responsible for IA



related training, operational procedures, documentation and business processes required to obtain and retain official accreditation of the online resources by full compliance of DoD Information Assurance Certification and Accreditation Process (DIACAP). This position requires DoD 8570.01 – M – IAM Level II qualification.

- Subcontractor Manager.
- Financial Manager.
- Contract Administrator.

This team shall be responsible for all services delivered; the management of subcontractors; and supervise development and implementation of MOS overall.

7.1.1 The Contractor shall develop and maintain a training program and methodology to ensure staff members remain proficient on military services specific issues and understand military terminology and the issues facing Service men and women and their dependents.

7.1.2 The Contractor shall develop and maintain management processes, tools and technical expertise to integrate all elements of the MOS requirements to support and maintain a system of counselors and care managers at a level of readiness over the contract's period of performance.

7.1.3 The Contractor shall develop and maintain processes and procedures to support the warm hand-off of Clients to other providers and community resources.

7.1.4 The Contractor shall develop and maintain management processes and procedures to provide services to Clients worldwide.

7.1.5 Contractor shall develop and maintain management processes to provide back up call center support.

7.1.6 The Contractor shall develop and maintain established management processes and procedures to meet peak usage periods and manage spikes in call volume.

7.1.7 The Contractor shall develop and maintain established processes and procedures for its obligations as it applies to "Duty to Warn" in the event a Client reveals a threat to self or others.

7.1.8 The Contractor shall develop and maintain established processes and procedures for meeting the staffing requirements including hiring, training, and managing a staff of Masters level professionals.

7.1.9 The Contractor shall develop and maintain management process to meet Section 508 of Workforce Investment Act of 1998 and all DoD security requirements as applicable.

7.1.10 The Contractor shall develop and maintain a process for regular updating and posting of Military and community quality of life information.

## **7.2 MOS STRATEGIC OUTREACH OBJECTIVE**

Strategic outreach materials and plans will raise awareness and further brand MOS for eligible populations with the main emphasis focused on Service members and their families, military leaders and service providers. Educational, informational and promotional materials provide Clients with in-depth information and resources that support Client management of the challenges of military and family life.

## **7.2.1 MINIMUM REQUIREMENTS FOR MOS STRATEGIC OUTREACH**

When directed by the Government MOS Program Office, the Contractor shall assist DoD in developing and implementing strategic outreach plans and materials (educational, informational and promotional) to support DoD program and priority areas. Government program areas for Strategic Outreach support include, but are not limited to: Family Support, Children and Youth, Family Advocacy, Families with Special Needs, Careers and Education, Deployment, Recreation, and Financial.

7.2.1.1 The Contractor shall provide educational and informational materials and referral information normally provided as part of the EAP support services.

7.2.1.2 As directed by the Government MOS Program Office, the Contractor shall provide MOS support to a small number of special events per month, which are not considered to be part of the JFSAP Program. These special events may consist of a staff person operating a booth with MOS outreach materials and answering questions about the MOS program or, in other cases, may require that only MOS outreach materials be sent to support the event.

7.2.1.3 The Contractor will provide the Government with monthly reports to identify trends in call center and counseling data. When directed by the Government MOS Program Office, the Contractor will assist the Government with analysis of this data to assess requirements for outreach materials (educational, informational and promotional) and plans.

7.2.1.4 When directed by the Government MOS Program Office, the Contractor shall develop or acquire outreach materials (pamphlets, books, CDs, games, etc.) to include DoD program materials that relate to the full range of MOS services and the issues of specific interest to Service members and families.

7.2.1.5 The Contractor shall have the capability to develop and distribute targeted informational materials to meet national or command level crisis or emergency needs, e.g. hostage situations, epidemics, natural disasters, etc. When directed by the Government MOS Program Office, the Contractor shall develop and distribute crisis response materials within 24 hours of the request.

7.2.1.6 As directed by the Government MOS Program Office, the Contractor shall review and update outreach materials and plans to maintain relevance and accuracy.

7.2.1.7 The Government will specify appropriate quarterly and monthly themes for strategic outreach. Examples of these themes and quarterly designations are:

- January – April: Financial Readiness, Taxes, Prevention of Identify Theft, Health and Wellness, Relocation
- May – July: Family, Military Family Month (May), Summer Recreation, Military Recreation Opportunities
- August – September: School and Education, Child Care, Spouse Careers and Education, Community Involvement, Consumer Awareness
- October – December: Holidays, Healthy Habits, Stress Reduction, Managing Military-Related Change

7.2.1.8 Strategic outreach plans shall include all Government approved media channels and venues. When directed by the Government MOS Program Office to support monthly and quarterly themes, the Contractor will prepare material for the Government to post to these venues. The venues include, but are not limited to:

- Armed Forces Press Service
- Defense Media Activity
- Government sponsored media events (Bloggers' Roundtable, Blog Posts on Government websites)
- Government managed Social Media pages to include, but not limited to Facebook,
- Twitter, YouTube

7.2.1.9 The Contractor will warehouse, provide inventory management and worldwide distribution services for all outreach materials to include, but not limited to:

- All EAP provided outreach materials (pamphlets, books, CDs, games, etc.)
- All existing Government owned MOS outreach materials (The Contractor will be provided a current inventory of Government owned outreach materials.)
- All Government developed or purchased outreach materials specified by the Government.
- Outreach materials provided to military Service members and their families through an MOU or MOA with the Government as specified by the Government.

7.2.1.10 The distribution services will allow clients to order fulfillment materials through either the MOS toll-free telephone number, the MOS Website or download the requested materials electronically. The Contractor shall ship materials to Clients within 2 business days from the receipt of request.

7.2.1.11 As directed by the Government MOS Program Office , the Contractor will replenish inventory.

7.2.1.12 Any material costs for strategic outreach must be approved in writing by the COR.

### **7.3 QUALITY ASSURANCE OBJECTIVE**

To ensure MOS Clients receive the highest quality services possible.

#### **7.3.1 MINIMUM REQUIREMENTS FOR QUALITY ASSURANCE**

The Contractor shall develop, implement and maintain a Quality Assurance Program for MOS EAP operations.

7.3.1.1 The Quality Assurance Program for all non-medical counseling programs will be consistent with the Council on Accreditation standards. The Contractor shall be able to demonstrate (at any time) to Government MOS Program Office or the CO, in writing, that the MOS staff and network providers are providing appropriate non-medical counseling support to Service members and their families.

7.3.1.2 The Contractor shall identify within the Quality Control Plan the measures necessary for monitoring performance for all MOS operations.

7.3.1.3 The Contractor shall maintain and provide all records and reports pertaining to quality assurance documentation for the life of this contract, and make them available for government review at any time during performance.

7.3.1.4 The Contractor will identify components for Quality Control that will ensure highest performance delivery of non-medical counseling services.

7.3. 1.5 The Contractor will identify a Quality Control support team that will ensure delivery of performance of non-medical counseling services.

7.3.1.6 The network shall be sufficient to ensure Client waiting periods for access to counselors do not extend beyond the requirements of this PWS.

#### **7.4 MILITARY ONESOURCE PROGRAM TRANSITION OUT**

The Contractor shall provide a 90 day plan that demonstrates the contractor's capacity and capability for an orderly and seamless transition out of the MOS Program.

7.4.1 The Transition Plan shall discuss the process for transferring services and associated data.

7.4.2 The Transition Plan shall identify quality assurance measures that will allow the Government to exercise its responsibilities for monitoring contractor performance. In addition, the Contractor shall identify any transition risk factors and plans for managing those risk factors.

7.4.3 Transition Reporting Requirements – Every two weeks, the contractor shall provide a report, in contractor format, detailing the status of milestones for call center, reports, disaster recovery, general education/materials, all non-medical counseling, all MOS centers, and all program oversight elements to include status of sub-contracts. As needed, a face to face update meeting will take place at the CO's location in Herndon, Virginia.

**Section D - Packaging and Marking**

**This section is intentionally left blank.**

## **SECTION E – INSPECTION AND ACCEPTANCE**

### **52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)**

The following contract clauses pertinent to this section are hereby incorporated by reference in accordance with the clauses at FAR “52.252-2 Clauses Incorporated by Reference” in Section I of this contract. This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. The full text of a clause may be accessed electronically at this address: <http://farsite.hill.af mil/vffar1.htm>

52.246-4	Inspection Of Services--Fixed Price	AUG 1996
52.246-6	Inspection--Time-And-Material And Labor-Hour	MAY 2001

#### **E.1 Inspection and Acceptance - Services**

Inspection, acceptance, and rejection will be based upon compliance with the contract Performance Work Statement (PWS) requirements. Payment constitutes acceptance and will be made in accordance with FAR 52.232-25, Prompt Payment.

Inspection of services to be furnished hereunder shall be performed by the COR in accordance with Clauses 52.246-4 and 52.246-6 above, and any other provisions/clauses specified in this contract. The Government reserves the right to conduct any inspection and test it deems reasonably necessary to assure that the services provided conform to all aspects of the PWS and contract requirements. Final acceptance of deliverables and Progress Reports shall be made by the COR.

#### **E.2 Inspection and Acceptance Criteria**

Final inspection and acceptance of all work performed, reports and other deliverables will be performed by the COR at the place of delivery. The basis for acceptance shall be compliance with the requirements and other terms and conditions of the contract. Deliverable items that are rejected shall be corrected in accordance with applicable clauses.

General quality measures as set forth below will be applied to each work product received from the contractor under the PWS.

- Work products shall be clear and concise. Any/all diagrams shall be easy to understand and be relevant to the supporting narrative.
- All text and diagrammatic files shall be editable by the Government.
- Work products shall be submitted on or before the due date specified in the PWS/deliverables table or submitted in accordance with a later scheduled date determined by the Government.

**SECTION F - DELIVERIES OR PERFORMANCE****F.1 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)**

The following contract clauses pertinent to this section are hereby incorporated by reference in accordance with the clauses at FAR "52.252-2 Clauses Incorporated by Reference" in Section I of this contract. This contract incorporates one or more clauses by reference, with the same force and effect as if they were provided in full text. The full text of a clause may be accessed electronically at the following address: <http://farsite.hill.af.mil/vffar1.htm>

52.242-15	Stop-Work Order	AUG 1989
52.242-17	Government Delay Of Work	APR 1984

**F.2 Period of Performance**

The term of this contract is as follows:

Base Period:	5 months
Option Period # 1:	From the end of the Base Period through 3 months.
Option Period # 2:	From the end of Option Period # 1 through 3 months.

**F.3 Place of Performance**

The anticipated places of performance may include the contractor site(s) as well as sites identified through ongoing assessments of client needs by the contractor and with the concurrence of the COR during performance of this effort. The places of performance include, but are not limited to, the contractor's office and locations throughout the U.S.

**F.4 Deliverables**

	<b><u>PWS Deliverables</u></b>	<b><u>Delivery</u></b>
1	The Contractor shall provide status on usage, by month and cumulative, for state and federal filings.	Monthly on 15th
2	The Contractor shall provide records and reports that document Client satisfaction and utilization levels. Reports shall also contain breakouts of the types of problems for which service members and their families are seeking assistance.	Monthly on 15 <sup>th</sup>
3	The Contractor shall submit and maintain protocols and procedures for assessment, referral, and case management of Clients in need of non-medical counseling services.	Upon award and within 5 days of any changes
4	The Contractor shall capture contact information in a database/s and provide reports detailing non-medical counseling services.	Monthly on 15 <sup>th</sup>
5	Contractor shall provide case files in an ASCII format.	Within 15 days of contract completion
6	Call Center Statistics Report	Monthly on the 15th
7	Call-Out Center Statistics	Monthly on the 15th
8	Manning or Staffing Report by Activity	Monthly on the 15th
9	The Contractor shall certify and be able to demonstrate to the Government MOS Program Office and the Contracting Officer (CO), in writing, that the non-medical counseling providers' and supervisors' licensure, credentials, required experience and background checks are current and proper for performance under this contract.	Upon award and prior to the exercise of each option period

## **F.5 Compliance**

The contractor must comply with all of the following requirements:

- (1) DoD Education Activity Schools requirements
- (2) DoDD No. 5200.2, DoD Personnel Security Program
- (3) DoDD No. 8910.01, Information Collection and Reporting
- (4) DoDI 1342.27, Personal Financial Management for Service Members
- (5) DoD Directive 6400.1, Family Advocacy Program
- (6) DoD Directives and Instructions related to Military Community and Family Programs
- (7) DSM (latest version) V-Codes
- (8) All other documents referenced in the PWS



## **SECTION G - CONTRACT ADMINISTRATION DATA**

### **G.1 Contracting Officer's Representative (COR)**

The COR for this effort is as follows:

ODUSD (MC&FP)  
John Schaefer  
Military Community and Family Policy  
Voice: 703-697-7191  
[John.Schaefer@osd.mil](mailto:John.Schaefer@osd.mil)

The OSD Program Manager for this effort is as follows:

ODUSD (MC&FP)  
David Kennedy  
Military Community and Family Policy  
Voice: 703-588-0059  
[David.Kennedy@osd.mil](mailto:David.Kennedy@osd.mil)

The COR is the individual within the Program Management function who has overall technical responsibility for this effort. The COR supports the Contracting Officer (CO) and Contract Administrator (CA) during administration of this effort by:

- 1) Making final decisions regarding any recommended rejection of deliverables;
- 2) Providing technical clarification relative to overall workload matters;
- 3) Providing advice and guidance to the Contractor in the preparation of deliverables and services;
- 4) Providing acceptance of deliverable products to assure compliance with requirements.

The COR also provides technical direction to the Contractor, i.e., shifting work emphasis between areas of work; fills in details, or otherwise serves to accomplish the purpose of this effort. Technical direction shall be within the general PWS for this effort. The COR does NOT have the authority to and may NOT issue any technical direction which:

- 1) Constitutes an assignment of work outside the general scope of this effort;
- 2) Constitutes a change as defined in the "Changes" clause;
- 3) In any way causes an increase or decrease in cost or the time required for performance;
- 4) Changes any of the terms, conditions, or other requirements of this effort; and
- 5) Suspends or terminates any portion of this effort.

All technical direction shall be issued in writing by the COR or will be confirmed by the COR in writing within 10 calendar days after verbal issuance. A copy of the written direction shall be furnished to the CO and the CA.

In addition to providing technical direction, the COR will:

- 1) Monitor the Contractor's technical progress, including surveillance and assessment of performance, and recommend to the CO and CA, any changes in the requirement;
- 2) Assist the Contractor in the resolution of technical problems encountered during performance; and
- 3) Perform inspection and acceptance or recommendation for rejection of Contractor deliverables and identify deficiencies in delivered items. This does not replace any other quality assurance inspection requirements that are specified elsewhere within the PWS.

If in the opinion of the Contractor, any instruction or direction issued by the COR is outside of his/her specific authority, the Contractor shall not proceed but shall notify the CO in writing within 5 working days after receipt of any instruction or direction, with an informational copy to the CA.

## **G.2 Contracting Officer (CO) Authority**

The CO is:

William Galvin  
Acquisition Services Directorate-Herndon  
Interior Business Center  
Department of Interior  
381 Elden St., Suite 4000  
Herndon, VA 20170  
Voice: 703-964-3690  
Email: William\_Galvin@nbc.gov

The CA is:

Christopher Morningstar  
Acquisition Services Directorate-Herndon  
Interior Business Center  
Department of Interior  
381 Elden St., Suite 4000  
Herndon, VA 20170  
Voice: 703-964-8444  
Email: Christopher\_S\_Morningstar@nbc.gov

In no event shall any understanding or agreement between the Contractor and any Government employee other than the CO on any contract modification, change order, letter or verbal direction to the Contractor be effective or binding upon the Government. All such actions must be formalized by a proper contractual document executed by an appointed CO. The Contractor is hereby put on notice that in the event a Government employee, other than the CO, directs a change in the work to be performed or increases the scope of work to be performed, it is the Contractor's responsibility to make inquiry of the CO before making the deviation. Payments will not be made without being authorized by an appointed CO with the legal authority to bind the Government.

### **G.3 Government Representatives**

The contract will be administered by an authorized representative of the CO. In no event, however, will any understanding or agreement, modification, change order, or other matter deviating from the terms and conditions of the contract between the Contractor and any person other than the CO be effective or binding upon the Government, unless formalized by proper contractual documents executed by the CO.

The COR is designated by the CO as the authorized representative of the CO. The COR is responsible for monitoring performance and technical management of the effort required hereunder, and should be contacted regarding questions or problems of a technical nature.

### **G.4 Notice to Government of Delay**

Whenever the contractor has knowledge that any actual or potential situation is delaying or threatens to delay the timely performance of this contract, the contractor shall, within 10 days, give written notice including all relevant information to the CO.

### **G.5 Project Management and Control**

The contractor shall designate a corporate officer with responsibility for personnel assignments and management control of all projects under this contract and a contract administrator responsible for project accounting and invoicing.

### **G.6 Submission of Invoices – Internet Payment Platform (IPP)**

Hardcopy invoices shall not be accepted, unless requested by the CO or the AQD Invoice Team.

#### **Electronic Invoicing and Payment Requirements (September 2011)**

Payment requests must be submitted electronically through the U. S. Department of the Treasury's IPP system.

"Payment request" means any request for contract financing payment or invoice payment by the Contractor. To constitute a proper invoice, the payment request must comply with the requirements identified in the applicable Prompt Payment clause included in the contract, or the clause 52.212-4 Contract Terms and Conditions – Commercial Items included in commercial item contracts. The IPP website address is: <https://www.ipp.gov>.

Under this contract, the following documents are required to be submitted as an attachment to the IPP invoice for Labor-Hour/Time-and-Materials CLINs:

1. Employee(s) Name(s)
2. Time Period Covered
3. Productive Direct Labor Hours for the current billing period and cumulative to date
4. Labor Category(s)
5. Hourly Rate
6. Any Travel or Other Direct Costs (ODCs) incurred (including supporting documentation/receipts for all charges) for the billing period and cumulative to date
7. The CLIN being invoiced

The Contractor must use the IPP website to register, access, and use IPP for submitting requests for payment. The Contractor Government Business Point of Contact (as listed in CCR and/or SAM) will receive enrollment instructions via email from the Federal Reserve Bank of Boston (FRBB) within 3 – 5 business days of the contract award date. Contractor assistance with enrollment can be obtained by contacting the IPP Production Helpdesk via email [ippgroup@bos.frb.org](mailto:ippgroup@bos.frb.org) or phone (866) 973-3131.

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

### **H.1 Transition Requirements**

Federal Acquisition Regulation (FAR) 52.237-3 “Continuity of Services,” as listed in Section I of this contract, may be used to accomplish the transition-out requirements of Section C, Paragraph 7.4 entitled, “Military OneSource Program Transition Out.” When notified by the Contracting Officer (CO), the Contractor shall implement the transition-out plan priced as CLIN 0010. The transition-out requirements must be accomplished within 90 days of that notification.

### **H.2 Save Harmless and Indemnity**

The Contractor shall save harmless and provide indemnity to the Government against any and all liability, claims, and costs of whatever kind and nature for injury or death of any person or persons and loss of damage to any property (Government or otherwise) occurring in connection with or in any incident to or arising out of the performance of work in connection with this contract, resulting in whole or in part from the negligent acts or omissions of the Contractor or subcontractor, or any employee, agent, or representative of the Contractor or subcontractor.

### **H.3 Clause Modifications**

Due to potential unforeseen circumstances attributable to the requirements solicited under this contract, the Government reserves the right to add, delete or modify clauses to facilitate specific conditions.

### **H.4 Conflict of Interest**

It is the Department of the Interior’s policy to avoid situations in the procurement process where, by virtue of work or services performed for DOI or DoD, or as the result of data acquired from DOI, DoD, or from industry, a particular company:

- a. Is given unfair competitive advantage over companies in respect to future DOI or DoD business;
- b. Is placed in a position to affect Government actions under circumstances in which there is danger that the company’s judgment may be biased; or
- c. Otherwise finds that a conflict exists between the performance of work or devices for Government in an impartial manner and the company’s self-interest.
- d. If the Contractor has reason to believe that a task assigned by the CO or a task being performed by the Contractor violates this policy, the Contractor shall promptly notify the CO in writing and state the reasons why a conflict of interest exists, or may appear to exist. After receiving such notice, the CO shall promptly inform the Contractor whether it should begin, or continue, the assigned task.
- e. Financial counselors shall provide service delivery that meets the standards in DODI 1342.27, and assist service members and their families with personal financial readiness. Regular reviews of Activity Reports and quality assurance reviews of financial services shall indicate that all financial counselors are practicing within the authorized scope of care.
- f. Further, the Contractor shall ensure that all personnel maintain the highest degree of sensitivity, compassion, and respect for service members and their families. The Contractor shall remain free of any political bias and shall ensure consistency of service regardless of installation, location, or any other factor.

## **H.5 Organizational and Consultant Conflict of Interest**

The Contractor shall insert the substance of this clause in all subcontracts.

a. It is recognized by the parties hereto that the effort performed by the Contractor under this contract is of a nature that it creates a potential organizational conflict of interest as contemplated under FAR 9.5.

b. In the performance of this contract, the Contractor may have access to data which is procurement sensitive or is proprietary to other companies, Government consultants or advisors, or the Government. The Contractor agrees that it will not utilize such procurement sensitive or proprietary data in performance of future competitive contracts. The Contractor further agrees not to act as a subcontractor or consultant to any other prime Contractor or subcontractor seeking to utilize such data.

c. The Contractor warrants that, to the best of its knowledge and belief, there are no relevant facts or circumstances, which would give rise to an organizational conflict of interest, as defined in FAR 9.5, or that the Contractor has disclosed all such relevant information.

d. The Contractor agrees that if an actual or potential organizational conflict of interest is discovered after award, the Contractor shall make a full disclosure in writing to the CO. This disclosure shall include a description of actions which the Contractor has taken or proposes to take to avoid or mitigate the actual or potential conflict.

e. If the Contractor was aware of a potential organizational conflict of interest prior to award or discovered an actual or potential conflict after award and did not disclose or misrepresented relevant information to the CO, the Government may terminate the Contract.

f. The Contractor/counselors shall remain free of any conflict of interest when issuing referrals to service members and their families. All personnel performing under this contract are expressly prohibited from self-referrals and referring service members and their families to any counseling practice for which the counselor may have a personal, financial or other interest.

## **H.6 Supervision of Contractor Employees**

a. Personnel assigned to render services under this contract shall be at all times under the direction and control of the Contractor. Notwithstanding any other provisions of this contract, the Contractor shall at all times be responsible for the supervision of its employees in the performance of the services required under this contract.

b. If the Contractor finds clarification necessary with respect to the scope of the services to be performed hereunder, he/she shall request in writing such clarification from the CO.

c. Contractor personnel shall not at any time during the contract period of performance be employees of the U.S. Government.

## **H.7 Removal of Contractor Personnel**

It is understood that all personnel assigned by the Contractor to the performance of work hereunder must be acceptable to the Government in terms of personal and professional conduct. Any person in the Contractor's organization, or in any subcontractor's organization, who is deemed by the CO or the COR to conflict with the interest of the Government, shall be immediately removed from this contract. Any security violations, denials or revocations of security clearance may be construed as grounds for immediate removal from the premises and the contract.

Further, the Government shall have the right to cause the Contractor to replace any individual who is determined by the Government to be a security risk, under the influence of alcohol or drugs, or is physically or mentally impaired to the extent that they cannot perform the tasks established by the contract. Such determination will be made at the sole discretion of the Military Service Headquarters Manager who will then report findings to OSD who will then subsequently report findings to the CO. Such determination shall not relieve the Contractor from meeting the performance requirements of this contract.

## **H.8 Notice To The Government of Delays**

In the event the Contractor encounters difficulty in meeting performance requirements, or when it anticipates difficulty in complying with the contract delivery schedule or date, or whenever the Contractor has knowledge that any actual or potential situation is delaying or threatens to delay the timely performance of this contract, the Contractor shall immediately notify the CO and the COR, in writing, giving pertinent details, provided, however, that this data shall be informational only in character and that this provision shall not be construed as a waiver by the Government of any delivery schedule or date or of any rights or remedies provided by law or under this contract.

## **H.9 Non-Payment for Additional Work**

Any additional services or a change to the work specified which may be performed by the Contractor, either at his/her own volition or at the request of an individual other than a duly appointed CO except as may be explicitly authorized in the contract, is not authorized and will not be paid for by DOI. Only a duly appointed CO is authorized to change the specifications, terms and conditions of this contract.

## **H.10 Key Personnel**

- a. The Contractor agrees to assign to the contract those key personnel whose resumes were submitted as required to fill the key position requirements. The Offeror may propose additional key positions to be fulfilled by key personnel. No substitution or addition of key personnel or addition/deletion of key positions will be made except in accordance with this clause.
- b. The Contractor agrees that to ensure continuity, personnel will remain on the project as long as they are employed with the company and performing satisfactorily. No personnel substitutions will be permitted, unless an individual's sudden illness, death, or termination of employment necessitates such substitutions. In any of these events, the Contractor must promptly notify the CO or COR in writing and provide the information required by paragraph (d) below.
- c. If key personnel, for whatever reason, become unavailable to work under this contract for a continuous period exceeding 30 working days, or are expected to devote, or are currently performing less effort to the work than indicated in its proposal, the Contractor must propose a substitution or reduction of effort of such personnel, in accordance with paragraph (d) below.
- d. All proposed key personnel substitutions or key position additions/deletions must be requested, in writing, to the CO and COR at least 15 days prior to the proposed change. Each request must provide a detailed explanation of the circumstances necessitating the proposed change, a complete resume from the proposed substitute and personnel to be replaced, and any other information required by the CO to approve or disapprove the proposed change. Resumes for key personnel substitutions or additions must be submitted in Contractor format, no longer than three pages, and signed by the individual and an authorized company representative certifying the accuracy of the information contained therein. All proposed substitutes (regardless of when they are proposed during the performance period) must have qualifications that are equal or higher than the qualifications of the person being replaced. No change in fixed unit prices may occur as a result of key personnel substitution.
- e. The CO will evaluate requests for substitutions and additions of personnel or positions and notify the Contractor, in writing, whether a request is approved or disapproved.
- f. The persons named below are considered to be key Contractor's personnel and essential for the successful completion of all work assigned under the contract.

<u>NAME</u>	<u>LABOR CATEGORY/POSITION</u>
Renee Owens Kennish	Program Director
Lucy Buckner	Deputy Program Director
Laura DeVault	Director of Call Center Operations
Jim Keener	Director of Non-Medical Counseling
Vince Connery	Director of Quality Control
Rachel Kaufmann	Director, Specialty Programs
Angelo Edge	Director of Information Technology Communication Resources
Izhar Mujaddidi	Information Security Manager
Tina Sarris	Financial Manager
John Sparks	Contract Administrator
Leah Dempsey	Subcontract Manager

#### **H.11 Permits and Licenses**

In performance of work under this contract, the Contractor must, without additional expense to the Government, be responsible for obtaining any necessary license(s) and permits, and for complying with all Federal, State, and municipal laws, codes, and regulations applicable to the performance of work. The Contractor shall verify all licensing, certification and/or compliance with industry accepted standards for the performance of non-medical counseling services.

#### **H.12 Confidentiality**

All information regarding the procedures developed under this contract must be regarded as sensitive information by the Contractor and not to be disclosed to anyone outside the Contractor's organization without the written authorization from the CO. Contractor personnel must sign a non-disclosure agreement before the initial start of work.

#### **H.13 Travel**

The Government anticipates that travel may be required in the performance of this contract. The Contractor is to include travel in the proposal, in sufficient detail for the Government to ensure that all requirements are included. Total travel will have a Not to Exceed (NTE) ceiling. No travel expenses submitted in excess of the NTE ceiling will be reimbursed without the written approval from the CO.

Travel by the Contractor's staff, including subcontractors, in support of this project will be reimbursed by DOI provided:

- 1) All travel must be approved, in writing and in advance by the COR. The Contractor's staff and subcontractors shall provide the COR adequate time to review and approve travel plans. The Government will not pay for any travel that is not approved in advance.
- 2) All travel and per diem charges must conform to the latest version of the Federal Travel Regulations (FTR) in effect at the time of travel authorization, including but not limited to, daily per diem and lodging rates in effect for the area at the time of the travel. Expenses not conforming to the FTR may be approved by the CO on a case by case basis upon receipt of adequate and sufficient explanation of the excess charges.
- 3) Costs incurred by Contractor personnel on official company business, whether foreign travel and/or domestic/local travel, are allowable, subject to the limitations contained in FAR 31.205-46 – Travel Costs Receipts and other written evidence to support submitted travel expenses shall be retained by the Contractor for the duration of the contract plus one year, and made available to the CO or COR on request. Travel not supported by receipts or other evidence will not be reimbursed and should not be submitted.

The Contractor shall state on all invoices that include claims for travel reimbursement that those claims are fully supported by proper documents, that the documents are available for audit, and that the claims confirm to the FTR.



## **H.14 Security**

**U.S. Citizenship:** Anyone working on the Military OneSource (MOS) Program must be a U.S. Citizen.

**Security Clearance:** A National Agency Check is required for the Counselors placed on military installations in performance of this contract.

**Security Requirements:** The Contractor is responsible for safeguarding information of a confidential or sensitive nature. Failure to safeguard any classified/privileged information, which may involve the contractor's personnel or to which they may have access to, may subject the contractor's employees to criminal liability under Title 18, section 793 of the United States Code. Provisions of the Privacy Act apply to all records and reports maintained by the contractor. All programs and materials developed at Government expense during the course of this contract are the property of the Government. As needed, Contractor personnel shall be required to obtain and maintain security badges. Contractor personnel will adhere to the security requirements of the different installation(s). The performance of this requirement will not require the Contractor to have access to classified information.

**The Common Access Card (CAC):** A CAC will be issued only when appropriate, in accordance with current guidance, and approved or requested at the installation level.

**Section 508 Compliance Requirements:** All electronic and information technology (EIT) procured through this effort must meet the applicable accessibility standards of 36 CFR 1194. 36 CFR 1194 implements Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d), and viewable at <http://www.section508.gov>.

**Access to DoD Information Systems:** Select individuals who require access to DoD information systems regardless of CLASSIFICATION level must be U.S. Citizens and obtain an External Certification Authority (ECA).

**Maintaining Privacy of Individual Records/Information.** The Contractor will be required to maintain (collect, maintain, use or disseminate) records or information about an individual that includes, but is not limited to, education, financial transactions, and employment history that contain their name or an identification system. In maintaining the privacy of the individuals, the Contractor shall comply with the Privacy Act of 1974, 5 U.S.C. 552a on maintaining records on individuals and the conditions of disclosure. Protect the records as "FOR OFFICIAL USE ONLY".

**Operations Security (OPSEC).** The Contractor, to include subcontractors, shall use the OPSEC process to protect "FOR OFFICIAL USE ONLY" and Privacy Act information under the MOS Program. This information is defined as controlled unclassified information obtained or generated as a result of MOS business operations. The Contractor/subcontractor shall not disclose controlled unclassified information to the public or any other organization outside of the MOS framework of providers without the written approval from the COR or the CO.

## **H.15 Standards**

Services shall adhere to the standards of practice set forth by relevant Service/DoD policies, federal, state, and local laws. The Contractor shall demonstrate sound professional judgment and the highest ethical standards in executing contract responsibilities.

## **H.16 Representation**

The Contractor shall not represent the Government at any federal, state, or military meeting or event.

## **H.17 Coordination and Communication**

The Contractor shall coordinate all program management, communication and service delivery through the COR and Government Program Manager.

#### **H.18 Contractor Attire**

Contractor personnel shall wear professional appropriate apparel, i.e., dresses, skirts, pants or slacks, shirt or blouse with collar and sleeves, shoes and socks. Tank-top shirts, cut-offs, shower shoes or similar items of apparel are prohibited. Clothing shall be clearly distinguishable from all U.S. Military Uniforms. Contractor personnel shall maintain a neat well-groomed appearance at all times to facilitate credibility with clients, staff, and command.

#### **H.19 Training**

Contractor personnel shall participate, as appropriate in locally available specialized training to maintain up-to-date knowledge and skills related to the military and civilian resources, database operation, and organizational structure. Attendance must be approved by the COR and the Military Service HQ POC.

#### **H.20 Small Business Participation Reporting and Compliance**

The contractor will meet or exceed small business (including ANCs and Indian tribes), veteran-owned small business, service-disabled veteran-owned small business, HUBZone small business, small disadvantaged business (including ANCs and Indian tribes), women-owned small business, and Ability One subcontracting goals proposed in response to the solicitation and throughout the period of performance of the resulting contract. The Government will audit compliance with the subcontracting goals proposed by the contractor.

#### **H.21 Subcontracting Compliance**

The Contractor understands and acknowledges that this requirement is a material part of the contract, and that failure to meet this requirement is a breach of contract, which can subject the Contractor to a termination for cause action. No later than 30 days prior to the conclusion of the current period, the Contractor shall provide a letter report to the CO showing how this requirement was met. Subcontracting goal attainment shall also be reported as part of the monthly report submitted to the Government.

#### **H.22 Electronic Transmission of Proprietary Data**

The successful Offeror shall be fully capable and willing to electronically transmit proprietary data to the Government. This data may consist of contract deliverables or pricing data required for proposal evaluation.

#### **H.23 Data Use, Disclosure of Information, and Handling of Sensitive Information**

The Contractor shall maintain, transmit, retain in strictest confidence, and prevent the unauthorized duplication, use, and disclosure of client information. The Contractor shall provide information only to the Government and contractors, to include all employees and subcontractors, having a need to know such information in the performance of their duties.

**23.1** The Contractor shall establish appropriate administrative and physical safeguards to ensure the security and confidentiality of client records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to the client.

**23.2** All contractors, to include employees and subcontractors, who will have access to client information will be advised of the confidential nature of the information, that records are subject to the requirements of the Privacy Act of 1974, and that unauthorized disclosure of client information may result in the imposition of possible criminal penalties.

**23.3** The Contractor agrees to assume responsibility for protecting the confidentiality of Government records, clients or otherwise, which are not public information.

**23.4** Information made available to the Contractor by the Government for the performance or administration of this contract shall be used only for those purposes and shall not be used in any other manner without the written agreement from the CO.

**23.5** If public information is provided to the Contractor for use in performance or administration of this contract, the contractor except with written permission from the CO, may not use such information for any other purpose. If the Contractor is uncertain about the availability or proposed use of information provided for the performance or administration, the Contractor will request, in writing, guidance from the COR and the CO regarding the use of the information for other purposes.

**23.6** The Contractor agrees to assume responsibility for protecting the confidentiality of Government records which are not public information. Each employee of the Contractor to whom information may be made available or disclosed shall be notified in writing by the Contractor that such information may be disclosed only for a specific purpose and extent authorized herein.

**23.7** Performance of this effort may require the contractor to access and use data/information proprietary to a Government agency or Government contractor which is of such nature that its dissemination or use, other than in performance of this contract, would be adverse to the interests of the Government and/or others.

**23.8** Contractor personnel shall not divulge or release data or information developed or obtained in performance of this contract, until made public by the Government, except to authorized Government personnel or upon written approval from the CO. The Contractor shall not use, disclose, or reproduce proprietary data that bears a restrictive legend, other than as required in the performance of this contract. Nothing herein shall preclude the use of any data independently acquired by the contractor without such limitations or prohibit an agreement at no cost to the Government between the Contractor and the data owner that provides for greater rights to the Contractor.

**23.9** All data received, processed, evaluated, loaded, and/or created shall remain the sole property of the Government unless specific exception is granted by the CO.

#### **H.24 Intellectual Property Rights**

The DoD shall receive *Unlimited Rights* in all intellectual property, including graphic/pictorial representations and text, created by the Contractor during performance of this contract.

#### **H.25 Ownership of MOS Logo, Web Address, 1-800 Telephone Number and Other MOS Related Materials**

The MOS logo, web address, open source web interface, all materials developed at the direction of the Government, the 1-800 telephone contact line and all MOS materials that are not used with the Contractor's civilian clients are considered property of the Government. The Contractor may retain use of such property as long as it is clearly understood that it is the Federal Government's property and the Federal Government has the right, at any time, to prohibit the Contractor from using such property and/or to order the Contractor to discontinue use of the property. The Contractor shall not use the property past the contract's period of performance.

#### **H.26 Services For This Agreement**

Any function or responsibility not specifically described in this Agreement but nevertheless considered an inherent part of services described and required for the proper performance and provision of EAP Services shall be deemed included for the purposes of this Agreement.

## **H.27 Post Award Evaluation of Contractor Performance**

### **2010-14 -- Amendment 1 -- Contractor Performance Assessment Reporting System – Notice to Contractors (CPARS)**

#### **Authorities and Delegations (July 2010)**

(a) FAR 42.1502 directs all Federal agencies to collect past performance information on contracts. The Department of the Interior (DOI) has implemented the Contractor Performance Assessment Reporting System (CPARS) to comply with this regulation. One or more past performance evaluations will be conducted in order to record your contract performance as required by FAR 42.15.

(b) The past performance evaluation process is totally paperless process using CPARS. CPARS is a web-based system that allows for electronic processing of the performance evaluation report. Once the report is processed, it is available in the Past Performance Information Retrieval System (PPIRS) for Government use in evaluation past performance as part of a source selection action.

(c) We request that you furnish the Contracting Officer with the name, position title, phone number, and email address for each person designated to have access to your firm's past performance evaluation(s) for the contract no later than 30 days after award. Each person granted access will have the ability to provide comments in the Contractor portion of the report and state whether or not the Contractor agrees with the evaluation, before returning the report to the Assessing Official. The report information must be protected as source selection sensitive information not releasable to the public.

(d) When your Contractor Representative(s) (Post Performance Points of Contract) are registered in CPARS, they will receive an automatically-generated email with detailed login instructions. Further details, systems requirements, and training information for CPARS is available at <http://www.cpars.csd.disa.mil/>. The CPARS User Manual, registration for On Line Training for Contractor Representatives, and a practice application may be found at this site.

(e) Within 60 days after the end of a performance period, the Contracting Officer will complete an interim or final past performance evaluation and the report will be accessible at <http://www.cpars.csd.disa.mil/>. Contractor Representatives may then provide comments in response to the evaluation, or return the evaluation without comment. Comments are limited to the space provided in Block 22. Your comments should focus on objective facts in the Assessing Official's narrative and should provide your views on the causes and ramifications of the assessed performance. In addition to the ratings and supporting narratives, blocks 1 – 17 should be reviewed for accuracy, as these include key fields that will be used by the Government to identify your firm in future source selection actions. If you elect not to provide comments, please acknowledge receipt of the evaluation by indicating "No comment" in Block 22, and then signing and dating Block 23 of the form. Without a statement in Block 22, you will be unable to sign and submit the evaluation back to the Government. If you do not sign and submit the CPARS within 30 days, it will automatically be returned to the Government and will be annotated: "The report was received by the contractor on (date). The contractor neither signed nor offered comment in response to this assessment". Your response is due within 30 calendar days after receipt of the CPAR.

(f) The following guidelines apply concerning your use of the past performance evaluation:

(1) Protect the evaluation as "source selection information". After review, transmit the evaluation by completing and submitting the form through CPARS. If for some reason you are unable to view and/or submit the form through CPARS, contact the Contracting Officer for instructions.

(2) Strictly control access to the evaluation within your organization. Ensure the evaluation is never released to persons or entities outside of your control.

(3) Prohibit the use of or reference to evaluation data for advertising, promotional material, pre award survey, responsibility determinations, production readiness reviews, or other similar purposes.

(g) If you wish to discuss a past performance evaluation, you should request a meeting in writing to the Contracting Officer no later than seven days following your receipt of the evaluation. The meeting will be held in person or via telephone or other means during your 30-day review period.

(h) A copy of the completed past performance evaluation will be available in CPARS for your viewing and for Government use supporting source selection actions after it has been finalized.

(End of notice)

#### **H. 28 Authorized Changes only by the CO**

(a) No order, statement, or conduct of Government personnel who visit the Contractor's facilities or in any other manner communicate with Contractor personnel during the performance of this contract shall constitute a change under the "Changes" clause of this contract.

(b) The Contractor shall not comply with any order, direction or request of Government personnel unless it is issued in writing and signed by the CO, or is pursuant to specific authority otherwise included as a part of this contract.

(c) The CO is the only person authorized to approve changes in any of the requirements of this contract, notwithstanding provisions contained elsewhere in this contract, the said authority remains solely the CO's. In the event the Contractor effects any change at the direction of any person other than the CO, the change will be considered to have been made without authority and no adjustment will be made in the contract price to cover any increase in charges incurred as a result thereof.

The address and telephone number of the CO is:

William Galvin  
381 Elden St., Suite 4000  
Herndon, VA 20170  
Phone: 703-964-3690  
E-mail: [William\\_Galvin@nbc.gov](mailto:William_Galvin@nbc.gov)

#### **H.29 Procedures for CLIN 0010 - Transition Out (Optional)**

The Government will exercise this Optional CLIN in the event that the MOS Program is awarded to a different Vendor. Since it is undetermined when the competitive contract will be awarded, this optional CLIN may be carried forward to any future period of performance (including option periods) within this contract. The contractor shall begin performance of this CLIN only upon written notice to proceed or modification of the contract. Prior to the issuance of a notice to proceed or modification, the Contractor agrees to negotiate, in good faith, with the Government a firm-fixed price to accomplish the transition of the MOS services.

**SECTION I – CONTRACT CLAUSES****52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)**

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this address: <http://farsite.hill.af.mil>

52.202-1	Definitions	JAN 2012
52.203-3	Gratuities	APR 1984
52.203-12	Limitation On Payments To Influence Certain Federal Transactions	OCT 2010
52.204-4	Printed or Copied Double-Sided on Recycled Paper	MAY 2011
52.204-7	Central Contractor Registration	AUG 2012
52.204-9	Personnel Identity Verification of Contractor Personnel	JAN 2011
52.209-6	Protecting the Government's Interest When Subcontracting With Contractors Debarred, Suspended, or Proposed for Debarment	DEC 2010
52.211-15	Defense Priority and Allocation Requirements	APR 2008
52.212-4	Contract Terms and Conditions—Commercial Items	FEB 2012
52.215-2	Audit and Records—Negotiation	OCT 2010
52.215-8	Order of Precedence—Uniform Contract Format	OCT 1997
52.215-21 Alt IV	Requirements for Cost or Pricing Data or Information Other Than Cost or Pricing Data—Modifications	OCT 2010
52.222-29	Notification of Visa Denial	JUN 2003
52.224-2	Privacy Act	APR 1984
52.227-1	Authorization and Consent	DEC 2007
52.227-2	Notice and Assistance Regarding Patent and Copyright Infringement	DEC 2007
52.227-17	Rights in Data – Special Works	DEC 2007
52.232-1	Payments	APR 1984
52.232-7	Payment Under Time-and-Materials and Labor Hour Contracts	AUG 2012
52.232-9	Limitation On Withholding Of Payments	APR 1984
52.232-11	Extras	APR 1984
52.232-18	Availability Of Funds	APR 1984
52.237-3	Continuity Of Services	JAN 1991
52.242-2	Production Progress Reports	APR 1991
52.242-13	Bankruptcy	JUL 1995
52.244-2	Subcontracts	OCT 2010
52.245-1 Alt I	Government Property	APR 2012
52.245-9	Use and Charges	APR 2012
52.246-20	Warranty of Services	MAY 2001
52.246-25	Limitation Of Liability—Services	FEB 1997
52.247-12	Supervision, Labor or Materials	APR 1984
52.247-21	Contractor Liability for Personal Injury and/or Property Damage	APR 1984
52.247-27	Contract Not Affected by Oral Agreement	APR 1984
52.249-2	Termination For Convenience Of The Government (Fixed-Price)	APR 2012
52.249-4	Termination for Convenience of the Government (Services) (Short Form)	APR 1984
52.249-8	Default (Fixed-Price Supply & Service)	APR 1984
52.249-14	Excusable Delays	APR 1984
52.251-1	Government Supply Sources	APR 2012
52.253-1	Computer Generated Forms	JAN 1991
252.201-7000	Contracting Officer's Representative	DEC 1991
252.204-7003	Control Of Government Personnel Work Product	APR 1992
252.204-7004 Alt A	Central Contractor Registration (52.204-7)	SEP 2007
252.205-7000	Provision Of Information To Cooperative Agreement Holders	DEC 1991
252.209-7004	Subcontracting With Firms That Are Owned or Controlled By The Government of a Terrorist Country	DEC 2006

252.219-7003	Small Business Subcontracting Plan (DoD Contracts)	AUG 2012
252.225-7001	Buy American Act And Balance Of Payments Program	JUN 2012
252.225-7002	Qualifying Country Sources As Subcontractors	JUN 2012
252.225-7004	Reporting of Contract Performance Outside the United States and Canada--Submission after Award	OCT 2010
252.225-7012	Preference For Certain Domestic Commodities	JUN 2012
252.225-7041	Correspondence in English	JUN 1997
252.225-7042	Authorization to Perform	APR 2003
252.227-7015	Technical Data--Commercial Items	DEC 2011
252.227-7016	Rights in Bid or Proposal Information	JAN 2011
252.227-7019	Validation of Asserted Restrictions--Computer Software	SEP 2011
252.227-7020	Rights in Special Works	JUN 1995
252.227-7021	Rights in Data--Existing Works	MAR 1979
252.227-7027	Deferred Ordering Of Technical Data Or Computer Software	APR 1988
252.227-7037	Validation of Restrictive Markings on Technical Data	JUN 2012
252.243-7001	Pricing Of Contract Modifications	DEC 1991
252.243-7002	Requests for Equitable Adjustment	MAR 1998

## CLAUSES INCORPORATED BY FULL TEXT

### 52.203-14 – Display of Hotline Poster(s).

#### Display of Hotline Poster(s) (Dec 2007)

(a) *Definition.*

“United States,” as used in this clause, means the 50 States, the District of Columbia, and outlying areas.

(b) *Display of fraud hotline poster(s).* Except as provided in paragraph (c)—

(1) During contract performance in the United States, the Contractor shall prominently display in common work areas within business segments performing work under this contract and at contract work sites—

(i) Any agency fraud hotline poster or Department of Homeland Security (DHS) fraud hotline poster identified in paragraph (b)(3) of this clause; and

(ii) Any DHS fraud hotline poster subsequently identified by the Contracting Officer.

(2) Additionally, if the Contractor maintains a company website as a method of providing information to employees, the Contractor shall display an electronic version of the poster(s) at the website.

(3) Any required posters may be obtained as follows:

Poster(s) Obtain from:

- 800-424-9098 or e-mail: [hotline@dodig.mil](mailto:hotline@dodig.mil)

- [http://www.dhs.gov/xoig/about/gc\\_1163703329805.shtm](http://www.dhs.gov/xoig/about/gc_1163703329805.shtm)

(c) If the Contractor has implemented a business ethics and conduct awareness program, including a reporting mechanism, such as a hotline poster, then the Contractor need not display any agency fraud hotline posters as required in paragraph (b) of this clause, other than any required DHS posters.

(d) *Subcontracts*. The Contractor shall include the substance of this clause, including this paragraph (d), in all subcontracts that exceed \$5,000,000, except when the subcontract—

(1) Is for the acquisition of a commercial item; or

(2) Is performed entirely outside the United States.

**52.212-5 -- Contract Terms and Conditions Required to Implement Statutes or Executive Orders -- Commercial Items (Aug 2012).**

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

(1) 52.222-50, Combating Trafficking in Persons (FEB 2009) (22 U.S.C. 7104(g)).

  X   Alternate I (AUG 2007) of 52.222-50 (22 U.S.C. 7104(g)).

(2) 52.233-3, Protest After Award (AUG 1996) (31 U.S.C. 3553).

(3) 52.233-4, Applicable Law for Breach of Contract Claim (OCT 2004) (Pub. L. 108-77, 108-78).

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the contracting officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

  X   (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (Sept 2006), with Alternate I (Oct 1995) (41 U.S.C. 253g and 10 U.S.C. 2402).

  X   (2) 52.203-13, Contractor Code of Business Ethics and Conduct (Apr 2010) (Pub. L. 110-252, Title VI, Chapter 1 (41 U.S.C. 251 note)).

       (3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (Jun 2010) (Section 1553 of Pub L. 111-5) (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009).

       (4) 52.204-10, Reporting Executive compensation and First-Tier Subcontract Awards (Aug 2012) (Pub. L. 109-282) (31 U.S.C. 6101 note).

       (5) 52.204-11, American Recovery and Reinvestment Act—Reporting Requirements (Jul 2010) (Pub. L. 111-5).

       (6) 52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment (Dec 2010) (31 U.S.C. 6101 note).



\_\_\_ (7) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (Feb 2012) (41 U.S.C. 2313).

\_\_\_ (8) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (May 2012) (section 738 of Division C of Public Law 112-74, section 740 of Division C of Pub. L. 111-117, section 743 of Division D of Pub. L. 111-8, and section 745 of Division D of Pub. L. 110-161).

\_\_\_ (9) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (Nov 2011) (15 U.S.C. 657a).

\_\_\_ (10) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (Jan 2011) (if the offeror elects to waive the preference, it shall so indicate in its offer)(15 U.S.C. 657a).

\_\_\_ (11) [Reserved]

\_\_\_ (12) (i) 52.219-6, Notice of Total Small Business Aside (Nov 2011) (15 U.S.C. 644).

\_\_\_ (ii) Alternate I (Nov 2011).

\_\_\_ (iii) Alternate II (Nov 2011).

\_\_\_ (13) (i) 52.219-7, Notice of Partial Small Business Set-Aside (June 2003) (15 U.S.C. 644).

\_\_\_ (ii) Alternate I (Oct 1995) of 52.219-7.

\_\_\_ (iii) Alternate II (Mar 2004) of 52.219-7.

X (14) 52.219-8, Utilization of Small Business Concerns (Jan 2011) (15 U.S.C. 637(d)(2) and (3)).

X (15) (i) 52.219-9, Small Business Subcontracting Plan (Jan 2011) (15 U.S.C. 637(d)(4).)

\_\_\_ (ii) Alternate I (Oct 2001) of 52.219-9.

X (iii) Alternate II (Oct 2001) of 52.219-9.

\_\_\_ (iv) Alternate III (July 2010) of 52.219-9.

\_\_\_ (16) 52.219-13, Notice of Set-Aside of Orders (Nov 2011) (15 U.S.C. 644(r)).

\_\_\_ (17) 52.219-14, Limitations on Subcontracting (Nov 2011) (15 U.S.C. 637(a)(14)).

X (18) 52.219-16, Liquidated Damages—Subcontracting Plan (Jan 1999) (15 U.S.C. 637(d)(4)(F)(i)).

\_\_\_ (19) (i) 52.219-23, Notice of Price Evaluation Adjustment for Small Disadvantaged Business Concerns (Oct 2008) (10 U.S.C. 2323) (if the offeror elects to waive the adjustment, it shall so indicate in its offer).

\_\_\_ (ii) Alternate I (June 2003) of 52.219-23.

\_\_\_ (20) 52.219-25, Small Disadvantaged Business Participation Program—Disadvantaged Status and Reporting (Dec 2010) (Pub. L. 103-355, section 7102, and 10 U.S.C. 2323).

\_\_\_ (21) 52.219-26, Small Disadvantaged Business Participation Program—Incentive Subcontracting (Oct 2000) (Pub. L. 103-355, section 7102, and 10 U.S.C. 2323).

\_\_\_ (22) 52.219-27, Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (Nov 2011) (15 U.S.C. 657f).

X (23) 52.219-28, Post Award Small Business Program Rerepresentation (Apr 2012) (15 U.S.C. 632(a)(2)).

\_\_\_ (24) 52.219-29, Notice of Set-Aside for Economically Disadvantaged Women-Owned Small Business (EDWOSB) Concerns (Apr 2012) (15 U.S.C. 637(m)).

\_\_\_ (25) 52.219-30, Notice of Set-Aside for Women-Owned Small Business (WOSB) Concerns Eligible Under the WOSB Program (Apr 2012) (15 U.S.C. 637(m)).

X (26) 52.222-3, Convict Labor (June 2003) (E.O. 11755).

X (27) 52.222-19, Child Labor—Cooperation with Authorities and Remedies (Mar 2012) (E.O. 13126).

X (28) 52.222-21, Prohibition of Segregated Facilities (Feb 1999).

X (29) 52.222-26, Equal Opportunity (Mar 2007) (E.O. 11246).

X (30) 52.222-35, Equal Opportunity for Veterans (Sep 2010) (38 U.S.C. 4212).

X (31) 52.222-36, Affirmative Action for Workers with Disabilities (Oct 2010) (29 U.S.C. 793).

X (32) 52.222-37, Employment Reports on Veterans (Sep 2010) (38 U.S.C. 4212).

\_\_\_ (33) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496).

X (34) 52.222-54, Employment Eligibility Verification (Jul 2012). (Executive Order 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial items as prescribed in 22.1803.)

\_\_\_ (35) (i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA-Designated Items (May 2008) (42 U.S.C. 6962(c)(3)(A)(ii)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

\_\_\_ (ii) Alternate I (May 2008) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

X (36) 52.223-15, Energy Efficiency in Energy-Consuming Products (Dec 2007) (42 U.S.C. 8259b).

\_\_\_ (37) (i) 52.223-16, IEEE 1680 Standard for the Environmental Assessment of Personal Computer Products (Dec 2007) (E.O. 13423).

\_\_\_ (ii) Alternate I (Dec 2007) of 52.223-16.

\_\_\_ (38) 52.223-18, Encouraging Contractor Policies to Ban Text Messaging while Driving (Aug 2011).

\_\_\_ (39) 52.225-1, Buy American Act--Supplies (Feb 2009) (41 U.S.C. 10a-10d).

\_\_\_ (40) (i) 52.225-3, Buy American Act--Free Trade Agreements--Israeli Trade Act (May 2012) (41 U.S.C. chapter 83, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, 19 U.S.C. 4001 note, Pub. L. 103-182, Pub. L. 108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-283, 110-138, 112-41, and 112-42).

\_\_\_ (ii) Alternate I (Mar 2012) of 52.225-3.

\_\_\_ (iii) Alternate II (Mar 2012) of 52.225-3.

\_\_\_ (iv) Alternate III (Mar 2012) of 52.225-3.

\_\_\_ (41) 52.225-5, Trade Agreements (May 2012) (19 U.S.C. 2501, *et seq.*, 19 U.S.C. 3301 note).

X (42) 52.225-13, Restrictions on Certain Foreign Purchases (Jun 2008) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).

\_\_\_ (43) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (Nov 2007) (42 U.S.C. 5150).

\_\_\_ (44) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov 2007) (42 U.S.C. 5150).

\_\_\_ (45) 52.232-29, Terms for Financing of Purchases of Commercial Items (Feb 2002) (41 U.S.C. 255(f), 10 U.S.C. 2307(f)).

\_\_\_ (46) 52.232-30, Installment Payments for Commercial Items (Oct 1995) (41 U.S.C. 255(f), 10 U.S.C. 2307(f)).

X (47) 52.232-33, Payment by Electronic Funds Transfer—Central Contractor Registration (Oct. 2003) (31 U.S.C. 3332).

\_\_\_ (48) 52.232-34, Payment by Electronic Funds Transfer—Other Than Central Contractor Registration (May 1999) (31 U.S.C. 3332).

\_\_\_ (49) 52.232-36, Payment by Third Party (Feb 2010) (31 U.S.C. 3332).

X (50) 52.239-1, Privacy or Security Safeguards (Aug 1996) (5 U.S.C. 552a).

\_\_\_ (51) (i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631).

\_\_\_ (ii) Alternate I (Apr 2003) of 52.247-64.

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or executive orders applicable to acquisitions of commercial items:

\_\_\_ (1) 52.222-41, Service Contract Act of 1965 (Nov 2007) (41 U.S.C. 351, *et seq.*).

\_\_\_ (2) 52.222-42, Statement of Equivalent Rates for Federal Hires (May 1989) (29 U.S.C. 206 and 41 U.S.C. 351, *et seq.*).

\_\_\_ (3) 52.222-43, Fair Labor Standards Act and Service Contract Act -- Price Adjustment (Multiple Year and Option Contracts) (Sep 2009) (29 U.S.C.206 and 41 U.S.C. 351, *et seq.*).

\_\_\_ (4) 52.222-44, Fair Labor Standards Act and Service Contract Act -- Price Adjustment (Sep 2009) (29 U.S.C. 206 and 41 U.S.C. 351, *et seq.*).

\_\_\_ (5) 52.222-51, Exemption from Application of the Service Contract Act to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (Nov 2007) (41 U.S.C. 351, *et seq.*).

\_\_\_ (6) 52.222-53, Exemption from Application of the Service Contract Act to Contracts for Certain Services--Requirements (Feb 2009) (41 U.S.C. 351, *et seq.*).

\_\_\_ (7) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations. (Mar 2009) (Pub. L. 110-247).

\_\_\_ (8) 52.237-11, Accepting and Dispensing of \$1 Coin (Sep 2008) (31 U.S.C. 5112(p)(1)).

(d) *Comptroller General Examination of Record* The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records -- Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to

appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(e)

(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c) and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in this paragraph (e)(1) in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause—

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (Apr 2010) (Pub. L. 110-252, Title VI, Chapter 1 (41 U.S.C. 251 note)).

(ii) 52.219-8, Utilization of Small Business Concerns (Dec 2010) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds \$650,000 (\$1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(iii) [Reserved]

(iv) 52.222-26, Equal Opportunity (Mar 2007) (E.O. 11246).

(v) 52.222-35, Equal Opportunity for Veterans (Sep 2010) (38 U.S.C. 4212).

(vi) 52.222-36, Affirmative Action for Workers with Disabilities (Oct 2010) (29 U.S.C. 793).

(vii) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.

(viii) 52.222-41, Service Contract Act of 1965, (Nov 2007), (41 U.S.C. 351, *et seq.*)

(ix) 52.222-50, Combating Trafficking in Persons (Feb 2009) (22 U.S.C. 7104(g)).

  X   Alternate I (Aug 2007) of 52.222-50 (22 U.S.C. 7104(g)).

(x) 52.222-51, Exemption from Application of the Service Contract Act to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (Nov 2007) (41 U.S.C. 351, *et seq.*)

(xi) 52.222-53, Exemption from Application of the Service Contract Act to Contracts for Certain Services--Requirements (Feb 2009) (41 U.S.C. 351, *et seq.*)

(xii) 52.222-54, Employment Eligibility Verification (Jul 2012).

(xiii) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations. (Mar 2009) (Pub. L. 110-247). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.

(xiv) 52.247-64, Preference for Privately-Owned U.S. Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(2) While not required, the contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

#### **52.217-6 OPTION FOR INCREASED QUANTITY (MAR 1989)**

The Government may increase the quantity of supplies called for in the Schedule at the unit price specified. The Contracting Officer may exercise the option by written notice to the Contractor within 7 days. Delivery of the added items shall continue at the same rate as the like items called for under the contract, unless the parties otherwise agree.

#### **52.217-7 OPTION FOR INCREASED QUANTITY— SEPARATELY PRICED LINE ITEM (MAR 1989)**

The Government may require the delivery of the numbered line item, identified in the Schedule as an option item, in the quantity and at the price stated in the Schedule. The Contracting Officer may exercise the option by written notice to the Contractor within 7 days. Delivery of added items shall continue at the same rate that like items are called for under the contract, unless the parties otherwise agree.

#### **52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)**

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 14 days.

#### **52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)**

(a) The Government may extend the term of this contract by written notice to the Contractor within 7 days, provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 14 days, before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed eleven-months of performance.

#### **52.224-1 PRIVACY ACT NOTIFICATION (JUL 1996) (DEVIATION)**

The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C.552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties. Applicable Department of the Interior regulations concerning the Privacy Act are set forth in 43 CFR 2, subpart D. The CFR is available for public inspection at the Departmental Library, Main Interior Bldg., 1849 C St. NW, Washington DC, at each of the regional offices of bureaus of the Department and at many public libraries.

**52.245-2 – GOVERNMENT PROPERTY INSTALLATION OPERATION SERVICES (APR 2012)**

(a) This Government Property listed in paragraph (e) of this clause is furnished to the Contractor in an “as-is, where is” condition. The Government makes no warranty regarding the suitability for use of the Government property specified in this contract. The Contractor shall be afforded the opportunity to inspect the Government property as specified in the solicitation.

(b) The Government bears no responsibility for repair or replacement of any lost, stolen, damaged or destroyed Government property. If any or all of the Government property is lost, stolen, damaged or destroyed or becomes no longer usable, the Contractor shall be responsible for replacement of the property at Contractor expense. The Contractor shall have title to all replacement property and shall continue to be responsible for contract performance.

(c) Unless the Contracting Officer determines otherwise, the Government abandons all rights and title to unserviceable and scrap property resulting from contract performance. Upon notification to the Contracting Officer, the Contractor shall remove such property from the Government premises and dispose of it at Contractor expense.

(d) Except as provided in this clause, Government property furnished under this contract shall be governed by the Government Property clause of this contract.

(e) Government property provided under this clause: Reference Section J, Attachment 6

**52.245-2 – AUTHORIZED DEVIATIONS IN CLAUSES (APR 1984)**

The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of “(DEVIATION)” after the date of the clause.

**252.204-7000 DISCLOSURE OF INFORMATION (DEC 1991)**

(a) The Contractor shall not release to anyone outside the Contractor's organization any unclassified information, regardless of medium (e.g., film, tape, document), pertaining to any part of this contract or any program related to this contract, unless—

(1) The Contracting Officer has given prior written approval; or

(2) The information is otherwise in the public domain before the date of release.

(b) Requests for approval shall identify the specific information to be released, the medium to be used, and the purpose for the release. The Contractor shall submit its request to the Contracting Officer at least 45 days before the proposed date for release.

(c) The Contractor agrees to include a similar requirement in each subcontract under this contract. Subcontractors shall submit requests for authorization to release through the prime contractor to the Contracting Officer.

**252.225-7043 ANTITERRORISM/FORCE PROTECTION POLICY FOR DEFENSE CONTRACTORS OUTSIDE THE UNITED STATES (MAR 2006)**

(a) Definition. United States, as used in this clause, means, the 50 States, the District of Columbia, and outlying areas.

(b) Except as provided in paragraph (c) of this clause, the Contractor and its subcontractors, if performing or traveling outside the United States under this contract, shall--

(1) Affiliate with the Overseas Security Advisory Council, if the Contractor or subcontractor is a U.S. entity;

(2) Ensure that Contractor and subcontractor personnel who are U.S. nationals and are in-country on a non-transitory basis, register with the U.S. Embassy, and that Contractor and subcontractor personnel who are third country nationals comply with any security related requirements of the Embassy of their nationality;

(3) Provide, to Contractor and subcontractor personnel, antiterrorism/force protection awareness information commensurate with that which the Department of Defense (DoD) provides to its military and civilian personnel and their families, to the extent such information can be made available prior to travel outside the United States; and

(4) Obtain and comply with the most current antiterrorism/force protection guidance for Contractor and subcontractor personnel.

(c) The requirements of this clause do not apply to any subcontractor that is--

(1) A foreign government;

(2) A representative of a foreign government; or

(3) A foreign corporation wholly owned by a foreign government.

(d) Information and guidance pertaining to DoD antiterrorism/force protection can be obtained from: **PGI 225.7403 Antiterrorism/force protection.**

#### **PGI 225.7403-1 General**

Information and guidance pertaining to DoD antiterrorism/force protection policy for contracts that require performance or travel outside the United States can be obtained from the following offices:

(1) For Army contracts: HQDA-AT; telephone, DSN 222-9832 or commercial (703) 692-9832.

(2) For Navy contracts: Naval Criminal Investigative Service (NCIS), Code 21; telephone, DSN 288-9077 or commercial (202) 433-9077.

(3) For Marine Corps contracts: CMC Code POS-10; telephone, DSN 224-4177 or commercial (703) 614-4177.

(4) For Air Force and Combatant Command contracts: The appropriate Antiterrorism Force Protection Office at the Command Headquarters. Also see <https://atep.dtic.mil>.

(5) For defense agency contracts: The appropriate agency security office.

(6) For additional information: Assistant Secretary of Defense for Special Operations and Low Intensity Conflict, ASD(SOLIC); telephone, DSN 227-7205 or commercial (703) 697-7205.

#### **252.232-7007 LIMITATION OF GOVERNMENT'S OBLIGATION (MAY 2006)**



(a) Contract line item(s) REFERENCE CLIN STRUCTURE are incrementally funded. For these item(s), the sum of REFERENCE CLIN STRUCTURE of the total price is presently available for payment and allotted to this contract. An allotment schedule is set forth in paragraph (j) of this clause.

(b) For item(s) identified in paragraph (a) of this clause, the Contractor agrees to perform up to the point at which the total amount payable by the Government, including reimbursement in the event of termination of those item(s) for the Government's convenience, approximates the total amount currently allotted to the contract. The Contractor is not authorized to continue work on those item(s) beyond that point. The Government will not be obligated in any event to reimburse the Contractor in excess of the amount allotted to the contract for those item(s) regardless of anything to the contrary in the clause entitled "Termination for Convenience of the Government." As used in this clause, the total amount payable by the Government in the event of termination of applicable contract line item(s) for convenience includes costs, profit, and estimated termination settlement costs for those item(s).

(c) Notwithstanding the dates specified in the allotment schedule in paragraph (j) of this clause, the Contractor will notify the Contracting Officer in writing at least ninety days prior to the date when, in the Contractor's best judgment, the work will reach the point at which the total amount payable by the Government, including any cost for termination for convenience, will approximate 85 percent of the total amount then allotted to the contract for performance of the applicable item(s). The notification will state (1) the estimated date when that point will be reached and (2) an estimate of additional funding, if any, needed to continue performance of applicable line items up to the next scheduled date for allotment of funds identified in paragraph (j) of this clause, or to a mutually agreed upon substitute date. The notification will also advise the Contracting Officer of the estimated amount of additional funds that will be required for the timely performance of the item(s) funded pursuant to this clause, for a subsequent period as may be specified in the allotment schedule in paragraph (j) of this clause or otherwise agreed to by the parties. If after such notification additional funds are not allotted by the date identified in the Contractor's notification, or by an agreed substitute date, the Contracting Officer will terminate any item(s) for which additional funds have not been allotted, pursuant to the clause of this contract entitled "Termination for Convenience of the Government."

(d) When additional funds are allotted for continued performance of the contract line item(s) identified in paragraph (a) of this clause, the parties will agree as to the period of contract performance which will be covered by the funds. The provisions of paragraphs (b) through (d) of this clause will apply in like manner to the additional allotted funds and agreed substitute date, and the contract will be modified accordingly.

(e) If, solely by reason of failure of the Government to allot additional funds, by the dates indicated below, in amounts sufficient for timely performance of the contract line item(s) identified in paragraph (a) of this clause, the Contractor incurs additional costs or is delayed in the performance of the work under this contract and if additional funds are allotted, an equitable adjustment will be made in the price or prices (including appropriate target, billing, and ceiling prices where applicable) of the item(s), or in the time of delivery, or both. Failure to agree to any such equitable adjustment hereunder will be a dispute concerning a question of fact within the meaning of the clause entitled "Disputes."

(f) The Government may at any time prior to termination allot additional funds for the performance of the contract line item(s) identified in paragraph (a) of this clause.

(g) The termination provisions of this clause do not limit the rights of the Government under the clause entitled "Default." The provisions of this clause are limited to the work and allotment of funds for the contract line item(s) set forth in paragraph (a) of this clause. This clause no longer applies once the contract is fully funded except with regard to the rights or obligations of the parties concerning equitable adjustments negotiated under paragraphs (d) and (e) of this clause.

(h) Nothing in this clause affects the right of the Government to terminate this contract pursuant to the clause of this contract entitled "Termination for Convenience of the Government."

(i) Nothing in this clause shall be construed as authorization of voluntary services whose acceptance is otherwise prohibited under 31 U.S.C. 1342.

(j) The parties contemplate that the Government will allot funds to this contract in accordance with the following schedule: REFERENCE CLIN STRUCTURE.

On execution of contract	\$
(month) (day), (year)	\$
(month) (day), (year)	\$
(month) (day), (year)	\$

**DIAR (Department of the Interior) CLAUSES:**

**1452.204-70 RELEASE OF CLAIMS – DEPARTMENT OF THE INTERIOR (JUL 1996)**

After completion of work and prior to final payment, the Contractor shall furnish the Contracting Officer with a release of claims against the United States relating to this contract. The Release of Claims form (DI-137) shall be used for this purpose. The form provides for exception of specified claims from operation of the release. The form may be found at: <http://www.doi.gov/nbc/formsmgt/forms/di137.pdf>.

**SECTION J - LIST OF DOCUMENTS, EXHIBITS AND OTHER****SECTION J TABLE OF CONTENTS**

<b>Document Type</b>	<b>Description</b>
Attachment 1	CLIN Structure
Attachment 2	Eligibility Matrix
Attachment 3	Glossary of Terms
Attachment 4	DoDD 5200.2 – DoD Personnel Security Program
Attachment 5	DoDI 8910.01 – Information Collection and Reporting
Attachment 6	Government Furnished Information and Property
Attachment 6A	Fulfillment Materials List
Attachment 7	Quality Assurance Surveillance Plan (QASP)
Attachment 8	Acronyms /Symbols
Attachment 9	National Defense Authorization Act (NDAA) of January 2008
Attachment 10	Languages
Attachment 11	Mandatory Compliance Requirements (PWS Appendix A)
Attachment 12	JFSAP Position Descriptions
Attachment 13	DoDI 1342.27 - Personal Financial Management for Service Members
Attachment 14	DoDI 1344.07 – Personal Commercial Solicitation on DoD Installations
Attachment 15	DoDD 6400.1 - Family Advocacy Program
Attachment 16	DoDD 8500.01E – Information Assurance
Attachment 17	DoDD 8570.01-M – Information Assurance Training, Certification, and Workforce Management
Attachment 18	DoDI 8510.01 – DoD Information Assurance Certification and Accreditation Process (DIACAP)
Attachment 19	DoDI 1402.5 – Criminal History Background Checks on Individuals in Child Care Services
Attachment 20	DoDI 6490.06 – Counseling Services for DoD Military, Guard and Reserve, Certain Affiliated Personnel, and Their Family Members
Attachment 21	Monthly Reporting Requirements

Attachment J-1		CLIN STRUCTURE						
ITEM #	Supplies/Services	CLIN Type	Quantity	Unit	Unit Price	Total	Funded Amount	Unfunded Amount
0001	1-800 Call Center Operations					\$ 13,301,382.00	\$ 7,319,262.80	\$ 5,982,119.20
0001A	Tier 1 Staffing Level -- Base Call Volume up to 20 000 Calls/Month	FFP	5	Months	Do Not Price	Do Not Price	Do Not Price	Do Not Price
0001B	Tier 2 Staffing Level -- Base Call Volume of approximately 20,001-30,000 Calls/Month	FFP	5	Months	Do Not Price	Do Not Price	Do Not Price	Do Not Price
0001C	Tier 3 Staffing Level -- Base Call Volume of approximately 30 001-40 000 Calls/Month	FFP	5	Months	Do Not Price	Do Not Price	Do Not Price	Do Not Price
0001D	Tier 4 Staffing Level -- Base Call Volume of approximately 40 001-50 000 Calls/Month	FFP	5	Months	\$ 1,410,882.60			
0001E	Tier 5 Staffing Level -- Base Call Volume of approximately 50,001-60,000 Calls/Month	FFP	5	Months	\$ 1,632,549.20			
0001F	Tier 6 Staffing Level -- Base Call Volume of approximately 60,001-70,000 Calls/Month	FFP	5	Months	\$ 1,829,815.70			
0001G	Tier 7 Staffing Level -- Base Call Volume of approximately 70 001-80 000 Calls/Month	FFP	5	Months	\$ 2,081,662.30			
0001H	Tier 8 Staffing Level -- Base Call Volume of approximately 80,001-90,000 Calls/Month	FFP	5	Months	\$ 2,259,799.30			
0001I	Tier 9 Staffing Level -- Base Call Volume of approximately 90,001-100,000 Calls/Month	FFP	5	Months	\$ 2,464,886.40			
0001J	Tier 10 Staffing Level -- Base Call Volume of approximately 100 001-110 000 Calls/Month	FFP	5	Months	\$ 2,660,276.40			
0001K	Tier 11 Staffing Level -- Base Call Volume of approximately 110,001-120,000 Calls/Month	FFP	5	Months	\$ 2,859,839.40			
0002	IT Operations Management	FFP	5	Months	\$ 359,758.06	\$ 1,798,790.30	\$ 1,798,790.30	\$ -
0003	Non-Medical Counseling	FFP		Session		\$ 8,724,392.25	\$ 8,724,392.25	\$ -
	Situational Counseling In Person		84,190	Session	\$ 92.46			
	Situational Counseling Telephonic/Electronic		5	Months	\$ 39,330.00			
	Financial Counseling In Person		195	Session	\$ 155.45			
	Financial Counseling Telephonic/Electronic		3,325	Session	\$ 54.94			
	Health & Wellness Coaching Telephonic/Electronic		5	Months	\$ 9,799.50			
	Tax Telephonic		8,765	Session	\$ 54.94			
0004	Mission Support Operations							
0004A	Joint Family Support Assistance Program (JFSAP)	FFP	5	Months	\$ 579,943.80	\$ 2,899,719.00	\$ 2,899,719.00	\$ -
0004B	Spouse Education and Career Opportunities (SECO)	T&M	3	Months	\$ 955,623.92	\$ 2,866,871.76	\$ 2,226,288.30	\$ 640,583.46
0005	Program Management	FFP	5	Months	\$ 367,624.65	\$ 1,838,123.25	\$ 1,838,123.25	\$ -
0006	Strategic Outreach -- Labor	T&M	5	Months	\$ 21,286.20	\$ 106,431.00	\$ 106,431.00	\$ -
0007	Facilities Lease and Operational Costs	FFP	5	Months	\$ 816,031.89	\$ 4,080,159.45	\$ 4,080,159.45	\$ -
0008	Other Direct Costs (ODCs - includes storage and freight)	Reimbursable	5	Months	\$ 353,969.89	\$ 1,769,849.45	\$ 1,769,849.45	\$ -
0009	Travel	Reimbursable	5	Months	\$ 47,396.84	\$ 236,984.20	\$ 236,984.20	\$ -
0010	Transition Out (Optional) - To be definitized after award	FFP	1	Job	\$ -	\$ -	\$ -	\$ -
BASE PERIOD TOTAL						\$ 37,622,702.66	\$ 31,000,000.00	\$ 6,622,702.66

# Military OneSource Eligibility Matrix

As of 5/23/2011

Population	Details & Description	MOS Online	Call Center Consultation & Services	Document Translation	Telephonic Translation	In-Person Non-Medical Counseling	Short-term Telephonic Non-Medical Counseling (STSF-T )	Online Non-Medical Counseling	Health Coaching Sessions	TAX	MyCAA
Active Duty (AD) Service Members (SM)	All active duty SMs.	X	X	X	X	X	X	X	X	X	
Reserve and Guard SMs	Members of the Army Reserve, Navy Reserve, Air Force Reserve, Air Force and Marine Corps Reserve of the United States (the DoD Reserve Components) regardless of activation status.	X	X	X	X	X	X	X	X	X	
Immediate Family of AD SMs	Immediate family includes spouses, children, and anyone who has legal responsibility for a SM's children during deployment or separation.	X	X	X	X	X	X	X	X	X	
Immediate Family of Reserve and Guard SMs	Immediate family includes spouses, children, and anyone who has legal responsibility for a SM's children during deployment or separation.	X	X	X	X	X	X	X	X	X	
Spouses of SMs E-1 to E-5, W-1, W-2, O-1, O-2	Spouses of Active Duty Service Members in paygrades E1-E5, W1-W2, and O1-O2; and Spouses of activated reserve SMs and National Guard in the same paygrades.	X	X	X	X	X	X	X	X	X	X
Survivors of deceased Service Members	Eligible regardless of cause of death of SM. Applies to Active Duty, Guard, and Reserve SMs regardless of activation status. For survivors, family includes: unremarried surviving spouse, children, parents, legal guardians, siblings, grandparents, and persons authorized to direct disposition of a SM's remains.	X	X	X	X	X	X	X	X	X	
Medically discharged SMs	Eligible if the service member is being serviced under one of the Services Wounded Warrior or Seriously Ill and Injured Programs.	X	X	X	X	X	X	X	X	X	
Immediate Family and Parents of Wounded Warrior/Seriously Injured	Eligible if the service member is being served under one of the Services Wounded Warrior or Seriously Ill and Injured Program. Immediate family includes spouses, children, and anyone who has legal responsibility for a SM's children during deployment or separation.	X	X	X	X	X	X	X	X	X	
TDRL	Service Members on Temporary Disability Retirement List (TDRL). Eligible until 180 days past End of Tour of Service (ETS), retirement date, or discharge date.)	X	X	X	X	X	X	X	X	X	

# Military OneSource Eligibility Matrix

As of 5/23/2011

Population	Details & Description	MOS Online	Call Center Consultation & Services	Document Translation	Telephonic Translation	In-Person Non-Medical Counseling	Short-term Telephonic Non-Medical Counseling (STSF-T )	Online Non-Medical Counseling	Health Coaching Sessions	TAX	MyCAA
Retired SMs and Immediate Family	Eligible until 180 days past End of Tour of Service (ETS), retirement date, or discharge date. Immediate family includes spouses, children, and anyone who has legal responsibility for a SM's children during deployment or separation.	X	X	X	X	X	X	X	X	X	
Discharged SMs and Immediate Family	Service members discharged honorably or general discharge and immediate family members. Eligible until 180 days past End of Tour of Service (ETS), retirement date, or discharge date.) Immediate family includes spouses, children, and anyone who has legal responsibility for a SM's children during deployment or separation.	X	X	X	X	X	X	X	X	X	
Caregivers (non-parent/non-spouse)	Caretakers and legal guardians of eligible SMs. Eligible for tax service if preparing SM's taxes.	X	X	X	X	X	X	X	X	X	
Members of the DoD Civilian Expeditionary Workforce	Eligible as defined by DoD Directive 1404.10 of 23 January 2009 when deployed. (DD Form 2365) Eligible during the 90 days prior to deployment and 180 days post-deployment.	X	X	X	X	X	X	X	X	X	
Immediate Family of DoD Civilian Expeditionary Workforce	Eligible as defined by DoD Directive 1404.10 of 23 January 2009 when deployed. (DD Form 2365) Eligible during the 90 days prior to deployment and 180 days post-deployment. Immediate family includes spouses, children, and anyone who has legal responsibility for a SM's children during deployment or separation.	X	X	X	X	X	X	X	X	X	
Non-military/non-spouses (e.g., partners; former spouses) who are the parent of a dependent child	Eligible if they are the parent of a <i>military dependent</i> - even if the services provided are not supporting the dependent directly.	X	X	X	X						

# Military OneSource Eligibility Matrix

As of 5/23/2011

Population	Details & Description	MOS Online	Call Center Consultation & Services	Document Translation	Telephonic Translation	In-Person Non-Medical Counseling	Short-term Telephonic Non-Medical Counseling (STSF-T )	Online Non-Medical Counseling	Health Coaching Sessions	TAX	MyCAA
DOD Civilians, National Guard, and Reserve Employees, Government Contractors, State civilians, contractors, and organizations	Employees who provide direct support to service members and military family members (Employees of Navy Fleet & Family Support Center; Army Community Services; Marine Corps Community Services; Air Force Family Readiness, and employees of DODEA, State JFHQ, Family Assistance Centers, Veteran Administration, American Legion, and Veteran of Foreign Wars, etc.). <b>Family members of the employee are not eligible.</b>	X	X	X	X						
Parent(s) and extended family members of Active Duty, Guard, or Reserve SMs	Eligible when needing assistance with issues that are directly related to their service member or on behalf of their service member. Extended family of SM includes: spouse, children, parents/legal guardians, siblings, grandparents, and persons authorized to conduct business on behalf of SM.	X	X								
Reserve Officers' Training Corps (ROTC)	Students enrolled in an accredited ROTC program, a college-based military officer commissioning program.	X	X								
Delayed Entry Recruit / "Future Recruits"	Individuals who have entered into a non-binding, but promissory contract with the Army, Navy, USMC or USAF (or appropriate Reserve/Guard component). Individuals who are not 18 years or older are required to have parental consent for selected services.	X	X								
Parent(s) and immediate family members of Delayed Entry Recruit / "Future Recruits"	Eligible when needing assistance with issues that are directly related to or on behalf of their "future recruit." Immediate family includes spouses, children, and anyone who has legal responsibility for a SM's children during deployment or separation.	X	X								
Military Academy Cadets	Students enrolled in service academies for Army, Navy, or Air Force.	X	X								
***Military OneSource reserves the right to grant exceptions to eligibility criteria and services outlined therein on a case by case basis***											

**Attachment 3**  
**Military OneSource Program**  
**Glossary of Terms**

<b>Term</b>	<b>Definition</b>
Addictive Relationships	Abuse and neglect; couples; divorce and separation; emotional aspects; family relationships
Anxiety	Separation anxiety; social anxiety; coping with anxiety; stress related anxiety; recognizing stress and anxiety in others and helping them cope
Anger	Anger management; controlling outbursts; preventative techniques; aggressive behavior
Assertiveness	Developing confidence; dealing with inferiority complex; learning to be more assertive
Binge Drinking	Warning signs; what to do when you suspect binge drinking;
Boyfriends/Girlfriends	Dealing with boyfriend/girlfriend relationships; adolescence and developing an interest in the opposite sex; puberty
Child Care	Parenting and child care issues; child care referrals (child care centers and family day care homes); child development; back up child care; separation anxiety
Children's Education	School locator; on-line homework centers; DoDEA link; on-line teacher training; etc.
Children and Youth	Child care center; family child care; before and after school care; pre-K; child care locator; summer child care; home alone; communicating with providers; paying for child care; extended hour care; occasional care; youth recreational activities; youth sponsorship, etc.
Conflict Resolution	Dealing with conflict; controlling aggression
Coping with Abuse	Victim advocacy; Duty to warn; Child Abuse/Neglect; Child Sexual Abuse; Domestic Abuse; Financial Neglect/Non-Support; Domestic Abuse Shelters; How & Where to Report Child Abuse; etc.
Counseling ("Need to Talk?")	Problem-solving counseling; educational sessions; surge; coaching support; etc.
Decision Making	Making tough decisions; considering consequences of decisions; making the right marriage decision during deployment situations; raising responsible decision-making children
Deployment Connections	Pre, During, Post Deployment; etc.



Deployment Stress	Coping with deployment; holiday stress and deployment; helping children understand and cope with deployment; return and reunion stress
Elder Care	Community resources; elder care locator; long-term care options; supporting the caregiver; etc.
Emotional Well-Being	Anxiety; depression; moodiness; relationships; emotional aspects of divorce/separation; personal growth; balancing work and life; coping with grief; suicide; violence and trauma
Family Relationships and Concerns	Building strong family bonds; managing single parenthood; non-traditional families; co-dependency in relationships; managing difficult teenagers; step families; staying connected; adoption; etc.
Financial Stability	Budget counseling; Money management; Banking; Credit management; Debt liquidation (Overcoming debt problems); Financial record keeping; Savings and Investments ; Government Insurance (example: SGLI); Management of special duty pays; Home Buying; and; Government Thrift Savings Plan
For Pet's Sake	Moving with pets; quarantine; training; how to choose the right pet; etc.
Friends/Roommates	Building strong friendships; making new friends as an adult; keeping in touch with friends; living with roommates
Healthy Habits	Link to TRICARE; stress management; diet; exercise; work/life balance; etc.
Homesickness	Coping with being away from home/loved ones; homesickness when deployed; homesickness when relocating
Individuation/Sense of Self	Self-esteem; building a sense of identity; understanding your value; etc.
Legal Matters	Link to legal assistance; wills; consumer issues; family law; etc.
Lifelong Learning (College, Scholarships)	Colleges and universities search; distance education locator; scholarship search; education loan information; tuition assistance; certification & licensing; etc.
Loss and Grief	Dealing with grief and loss; grief and loss after a traumatic event; coping with unresolved grief; managing performance during times of loss; helping children deal with loss; coping with the death of a spouse or family member
Making Friends	Making new friends; building strong friendships; developing friends from different cultures; etc.

Marital/Couples Issues	Maintaining strong relationships during times of deployment; marital stress; building trust; couples problem-solving counseling; couples and money; couples issues when living abroad; keeping communication lines open; growing as a couple in midlife; infertility; etc.
Military Hotels (Lodging)	Temporary housing facilities available for use by service members, dependents, and DoD civilian employees
Military 101	Service websites; benefits; etc.
Money Matters	Budgeting; Turbo Tax; TSP; budget worksheets; saving for retirement; aid societies; on-line calculators; mortgage; loans; credit cards; etc.
Parenting	Becoming a parent; adoption; children's health; school issues; communicating with children; balancing work and family; single parenting; discipline; loss/birth complications; pregnancy; infertility; child developmental stages; etc.
Parent-Child Communications	Talking to children about violence and war; listening to your children; verbal and non-verbal communications; helping children deal with deployment; talking to your teenager; talking to children about change; etc.
Perfectionism	Helping children deal with social and academic pressures; dealing with failure; managing expectations; etc.
Recreation (MWR)	Link to AFRTs; recreation opportunities; MWR; travel; etc.
School Work/Grades	Homework tips; study skills; tutoring; adjusting to a new school and new expectations; helping your child succeed in school
Self-Esteem/Independence	Building self-esteem; developing independence when a spouse is deployed; building a sense of identity; how to help your teenager become independent and self-motivated; building self-esteem as an adult; etc.
Serious Illness in Family	Coping with illness; talking to children about serious illness; dealing with a loved one who is terminally ill; etc.
Shopping and Services (Commissary/Exchanges)	Link to DECA and exchanges; etc.
Smooth Moves (Relocation)	SITES link; family relocation; making connections in a new community; planning a move; move checklist; know your neighborhood; families first; etc.

Social Issues	Becoming involved in your community; community service; building community as a single parent; volunteering and community involvement; awareness of social issues; etc.
Special Needs	Disabilities; education; special needs assistance; schools, etc.
Spouse Careers (Training & Education)	Job search; career assistance; resume posting; certification & licensure; scholarships; education (GED, college, graduate); etc.
Spouse Career Counseling	Personalized assessment/analysis of skills and interests; Assess training and education interests; Career exploration; Assist with resume writing; Guidance on use of Internet to obtain employment; Assist with professional credentialing and licensure requirements; Develop interview skills; Provide information on occupations and salaries; and Assist with career planning and transitions
Stress	Managing deployment stress; combat and operational stress; stress and depression; teenagers and stress; understanding and avoiding burnout; managing stress as a family; caregiver/support stress; etc.
Substance Abuse (Addiction and Recovery)	Alcohol and drugs; co-worker/friend/partner intervention; prevention; compulsive behaviors; etc.
Transition to Civilian Life	Transition to civilian life; VA issues; link to VA website; etc.
TRICARE	Military medical care system
Values/Life Meaning	“Why are we here”; religion and values; remaining true to your values; building good values in children; how your values can affect your children; teaching children to resist biases and prejudices



# Department of Defense DIRECTIVE

NUMBER 5200.2

April 9, 1999

---

---

ASD(C3I)

SUBJECT: DoD Personnel Security Program

- References:
- (a) DoD Directive 5200.2, subject as above, May 6, 1992 (hereby canceled)
  - (b) Executive Order 12968, "Access to Classified Information," August 2, 1995
  - (c) Section 781 of title 50, United States Code
  - (d) Sections 831 through 835 of title 50, United States Code
  - (e) Executive Order 10450, "Security Requirements for Government Employment," April 27, 1953
  - (f) Executive Order 12958, "Classified National Security Information," April 17, 1995
  - (g) through (q), see enclosure 1

## 1. REISSUANCE AND PURPOSE

This Directive:

1.1. Reissues reference (a) to update the policy and responsibilities for the DoD Personnel Security Program under references (b) through (h).

1.2. Continues to authorize the publication of DoD 5200.2-R (reference (i)) in accordance with DoD 5025.1-M (reference (j)).

## 2. APPLICABILITY

This Directive applies to:

2.1. The Office of the Secretary of Defense, the Military Departments (including the Coast Guard when it is operating as a Military Service in the Navy), the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

2.2. DoD civilian personnel, members of the Armed Forces (excluding the Coast Guard in peacetime), contractor personnel and other personnel affiliated with the Department of Defense. Except that the unfavorable administrative action procedures pertaining to contractor personnel requiring access to classified information are contained in DoD 5220.22-R (reference (k)) and in DoD Directive 5220.6 (reference (l)).

### 3. POLICY

It is DoD policy that:

3.1. The objective of the personnel security program is that military, civilian, and contractor personnel assigned to and retained in sensitive positions, in which they could potentially damage national security, are and remain reliable and trustworthy, and there is no reasonable basis for doubting their allegiance to the United States.

3.2. No person shall be appointed or retained as a civilian employee in a sensitive position of the Department of Defense, as provided in reference (e), accepted for entrance into the Armed Forces of the United States, or assigned to duties that require a personnel security investigation as provided in 3.9., below, unless such appointment, acceptance, or assignment is clearly consistent with the interests of national security.

3.3. No person shall be deemed to be eligible for access to classified information unless such access is clearly consistent with the interests of national security as provided for in reference (b). Eligibility for access shall not be granted merely by reason of Federal service or contracting, licensee, certificate holder, or grantee status, or as a matter of right or privilege, or as a result of any particular title, rank, position, or affiliation.

3.4. Except as provided in 3.6., below, eligibility for access to classified information or assignment to sensitive duties shall be granted only to individuals who are United States citizens for whom an appropriate investigation has been completed and whose personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound

judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information. However, in exceptional circumstances where official functions must be performed prior to completion of the investigative and adjudication process, temporary eligibility for access to classified information may be granted to an individual.

3.5. A determination of eligibility for access to classified information or assignment to sensitive duties is a discretionary security decision based on judgments by appropriately trained adjudicative personnel.

3.6. As an exception, a non-U.S. citizen may be assigned to sensitive duties or granted a Limited Access Authorization for access to classified information in support of a specific DoD program, project, or contract that cannot be filled by a cleared or clearable U.S. citizen provided it is approved by an authorized official (as specified in DoD 5200.2-R, reference (i)).

3.7. In determining eligibility for access to classified information, the Department of Defense may investigate and consider any matter that relates to the determination of whether access is clearly consistent with the interests of national security. No inference concerning the standard in paragraph 3.4., above, may be raised solely on the basis of the sexual orientation of the individual.

3.8. No negative inference may be raised solely on the basis of mental health counseling. Such counseling can be a positive factor in eligibility determinations. However, mental health counseling, where relevant to the adjudication of access to classified information, may justify further inquiry to determine whether the standards of paragraph 3.4., above, are satisfied, and mental health may be considered where it directly relates to those standards.

3.9. DoD 5200.2-R (reference (i)) shall identify those positions and duties that require a personnel security investigation (PSI). A PSI is required for:

3.9.1. Appointment to a sensitive civilian position.

3.9.2. Entry into military service.

3.9.3. The granting of a security clearance or approval for access to classified information.

3.9.4. Assignment to other duties that require a personnel security or trustworthiness determination.

3.9.5. Continuing eligibility for retention of a security clearance and approval for access to classified information or for assignment to other sensitive duties.

3.10. Reference (i) shall contain personnel security criteria and adjudicative guidance to assist in determining whether an individual meets the clearance and sensitive position standards referred to in paragraphs 3.2. and 3.4., above.

3.11. No unfavorable personnel security determination shall be made except in accordance with procedures set forth in reference (i); Director of Central Intelligence Directive 1/14 (DCID 1/14) (reference (m)); DoD Directive 5220.6 (reference (l)) or as otherwise authorized by law.

#### 4. RESPONSIBILITIES

4.1. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence shall:

4.1.1. Serve as the Department of Defense Senior Agency Official for the Personnel Security Program under Section 6.1(a) of E.O. 12968, reference (b) and Special Access Programs under Section 5.6(c)(1) of E.O. 12958, reference (f).

4.1.2. Direct, administer, and oversee the DoD Personnel Security Program to ensure that the program is consistent, cost-effective, and efficient, and balances the rights of individuals with the interests of national security.

4.1.3. Approve, when appropriate, requests for exceptions to the DoD Personnel Security Program, except for access to NATO classified information. Requests for exceptions, which involve access to NATO classified information shall be sent to the Deputy Undersecretary of Defense (Policy) for Policy Support.

4.1.4 Issue and maintain reference (i), consistent with DoD 5025.1-M (reference (j)).

4.1.5. Ensure that research is conducted to assess and improve the effectiveness of the DoD Personnel Security Program (DoD Directive 5210.79 (reference (n))).

4.1.6. Ensure that the Defense Security Service (DSS) is operated pursuant to DoD Directive 5105.42 (reference (o)).

4.1.7 Ensure that the DSS provides the education, training, and awareness support to the DoD Personnel Security Program under DoD Directive 5200.32 (reference (p)).

4.1.8 Ensure that the personnel security program at the National Security Agency is consistent with the requirements of 50 U.S.C. Sections 831-835 (reference (d) and reference (m)).

4.2. The General Counsel of the Department of Defense shall:

4.2.1. Be responsible for providing advice and guidance as to the legal sufficiency of procedures and standards implementing the DoD Personnel Security Program.

4.2.2. Exercise oversight of personnel security program appeals procedures to verify that the rights of individuals are being protected consistent with the Constitution, laws of the United States, Executive orders, Directives, or Regulations that implement the DoD Personnel Security Program, and with the interests of national security.

4.2.3. Perform such functions relating to the DoD Personnel Security Program in accordance with DoD Directive 5145.1 (reference (q)) as the Secretary or Deputy Secretary of Defense may assign.

4.3. The Heads of the DoD Components shall:

4.3.1. Designate a senior official who shall be responsible for implementing the DoD Personnel Security Program within their DoD Components.

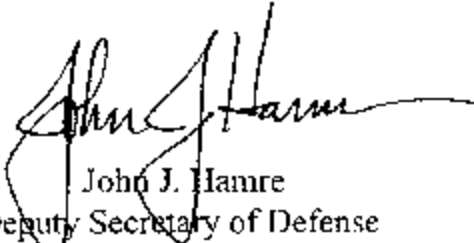
4.3.2. Ensure that the DoD Personnel Security Program is properly administered under this Directive within their DoD Components.

4.3.3. Ensure that information and recommendations on any aspect of this Directive and the DoD Personnel Security Program are provided to the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence.



5. EFFECTIVE DATE

This Directive is effective immediately.



John J. Hamre  
Deputy Secretary of Defense

Enclosures - 1

E1. References, continued

E1. ENCLOSURE 1

REFERENCES, continued

- (g) Executive Order 10865, "Safeguarding Classified Information Within Industry," February 20, 1960
- (h) Executive Order 12333, "United States Intelligence Activities," December 4, 1981
- (i) [DoD 5200.2-R](#), "Personnel Security Program," January 1987
- (j) [DoD 5025.1-M](#), "Department of Defense Directives System Procedures," August 1994
- (k) [DoD 5220.22-R](#), "Industrial Security Regulation," December 4, 1985
- (l) [DoD Directive 5220.6](#), "Defense Industrial Personnel Security Clearance Review Program," January 2, 1992
- (m) Director of Central Intelligence Directive 1/14, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)," July 2, 1998
- (n) [DoD Directive 5210.79](#), "Defense Personnel Security Research Center (PERSEREC)," July 9, 1992
- (o) [DoD Directive 5105.42](#), "Defense Investigative Service," June 14, 1985
- (p) [DoD Directive 5200.32](#), "Department of Defense Security Countermeasures (SCM) and Polygraph Education, Training, and Program Support," February 26, 1996
- (q) [DoD Directive 5145.1](#), "General Counsel of the Department of Defense," December 15, 1989



# Department of Defense

## INSTRUCTION

NUMBER 8910.01

March 6, 2007

---

---

ASD(NII)/DoD CIO

SUBJECT: Information Collection and Reporting

- References:
- (a) DoD Directive 8910.1, "Management and Control of Information Requirements," June 11, 1993 (hereby canceled)
  - (b) Acting Deputy Secretary of Defense Memorandum, "DoD Directives Review – Phase II," July 13, 2005
  - (c) DoD Directive 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005
  - (d) Chapter 35 of title 44, United States Code
  - (e) through (n), see Enclosure 1

### 1. REISSUANCE AND PURPOSE

This Instruction:

- 1.1. Reissues Reference (a) as a DoD Instruction in accordance with the guidance in Reference (b) and the authority in Reference (c).
- 1.2. Establishes and reissues policies and assigns responsibilities for the collection of information and the control of the paperwork burden consistent with Reference (d).
- 1.3. Continues to authorize publication of DoD 8910.1-M, (Reference (e)) by the Director, Washington Headquarters Services (WHS), in accordance with DoD 5025.1-M (Reference (f)).

### 2. APPLICABILITY AND SCOPE

This Instruction applies to:

- 2.1. The Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other

organizational entities in the Department of Defense (hereafter referred to collectively as the "DoD Components").

2.2. Information collected from sources external to the Federal Government, as well as internally in the Department of Defense.

2.3. The collection of information to satisfy statutory, congressional, and approved interagency information requirements, and those in support of all management functions, unless excluded in Reference (e).

### 3. DEFINITIONS

Terms used in this Instruction are defined in Enclosure 2.

### 4. POLICY

It is DoD policy that:

4.1. Prior to collecting information, users requiring the information shall ensure that the information to be collected is not duplicative of information already available. When information is not already available, users shall ensure that:

4.1.1. Other methods (e.g., statistical sampling) that will minimize the information collection burden cannot be used.

4.1.2. The information collection request is valid, accurate, and essential to the mission of the user's organization.

4.2. Information collection requirements shall be designed to meet only essential needs and be as infrequent as feasible, with reasonable due dates. The number of copies to be prepared shall be held to a minimum. One-time information collection requirements may not be imposed when the need for a recurring information collection requirement is indicated.

4.3. Information collected from the public as defined in Reference (d), DoD Components, and other Federal Agencies shall be minimized, accounted for, and controlled.

4.3.1. Part 1320 of Title 5, Code of Federal Regulations (Reference (g)), directs that public information collections be submitted to the Office of Management and Budget (OMB) for approval and assigned an OMB control number, and that an annual information collection budget of burden hours be developed and submitted to the OMB.

4.3.2. Information collection requirements that are within the sponsoring DoD Component shall be approved and assigned a Component information control symbol.

4.3.3. DoD internal information requirements, where information across DoD Components is collected, shall be approved and assigned an information control symbol at the Office of Secretary of Defense (OSD) Component level. If the DoD Component is other than an OSD Component, the DoD Component must obtain an OSD sponsor.

4.3.4. Interagency information collection requirements, where the Department of Defense is the requesting agency, shall be approved and assigned an information control symbol at the OSD Component level.

4.4. Information collection requirements that have not been properly approved and symbolized shall not be honored.

4.5. Collections of information that contain personal information on individuals require special handling under DoD Directive 5400.11 (Reference (h)). Such information included in the proposed collection of information shall be accessible to the public, only as prescribed by DoD Directive 5400.7 (Reference (i)). To ensure personal information in electronic form is only acquired and maintained when necessary, and that the supporting information technology that is being developed and used protects and preserves the privacy of the American public, privacy impact assessments shall be conducted in accordance with DoD Privacy Impact Assessment (PIA) Guidance (Reference (j)).

4.6. When the information collection requirement has been approved and symbolized, and the information is collected, it shall be made visible, available, and usable to any potential authorized user.

## 5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO) shall, consistent with the guidance prescribed by OMB:

5.1.1. Develop and issue DoD-wide policies related to internal DoD, interagency, and public information collection activities.

5.1.2. Establish goals, consistent with critical mission needs, to reduce the number and frequency of OSD-prescribed internal information collection requirements.

5.1.3. Oversee the accomplishment of DoD information collection reduction goals.

5.1.4. Approve and issue the DoD information collection budget and monitor its execution.

5.2. The Under Secretary of Defense for Personnel and Readiness shall, before submission to the Director, WHS, approve surveys requiring participation of personnel in any DoD

Component, other than the sponsoring Component, as prescribed by DoD Instruction 1100.13 (Reference (k)).

5.3. The Director, WHS, shall:

5.3.1. Develop, coordinate, and publish Reference (e) consistent with the policies and guidance contained herein, and in accordance with Reference (f).

5.3.2. Establish an OSD information collection control activity to:

5.3.2.1. Maintain and distribute an index of approved information collections that is updated monthly on the WHS Information Management Division Web site located at: <http://www.dtic.mil/whs/directives/infomgt/imd.htm>.

5.3.2.2. Serve as the DoD clearance office and the office of record for DoD public information collection requirements, in accordance with References (d) and (g).

5.3.2.3. Serve as the office of record and approval authority for OSD-prescribed internal information collection requirements to include interagency collection requirements imposed by the Department of Defense, in accordance with guidance in References (d), (e), and (g), as well as 10 U.S.C. 1782 (Reference (l)), OMB Circular A-130 (Reference (m)), and this Instruction.

5.3.3. Process information collection requirements submitted by the OSD staff after the staff has performed an assessment of ongoing information collection requirements.

5.3.4. Develop and coordinate the information collection budget.

5.4. The Heads of DoD Components and the OSD Principal Staff Assistants shall:

5.4.1. Ensure that users justify new information collection requirements before submission for approval to ensure that the information is not already available from other sources. Ensure that data is not duplicated or unnecessarily generated to reduce costs.

5.4.1.1. Evaluate and screen each data element in an information collection requirement against information in existing information collection requirements to determine whether such existing information can satisfy the requirement.

5.4.1.2. Subject each new or revised information collection requirement to a cost analysis. An estimate or actual cost of obtaining the information shall be developed by the requester in accordance with Reference (e).

5.4.2. Determine whether the information is releasable from the Component to the other Federal Agencies.

5.4.3. Establish an information requirements control activity under the DoD Components' Chief Information Officer or representative to:

5.4.3.1. Serve as the principal point of contact on the various information collection requirements programs.

5.4.3.2. Ensure information collection requirements that include research involving human subjects are reviewed in accordance with the requirements of DoD Directive 3216.2, "Protection of Human Subjects and Adherence to Ethical Standards in DoD-Supported Research" (Reference (n)).

5.4.3.3. Provide for the efficient and effective management and control of information collection requirements.

5.4.3.4. Process, symbolize, and cancel DoD Component internal information collection requirements, where applicable. Ensure information control symbols assigned by a higher level shall not be assigned a different DoD Component information control symbol by a lower level organization.

5.4.3.5. Notify the office requesting the information that approval and the assignment of an information control symbol must be obtained before the information can be collected.

5.4.3.6. Submit respective information collection budgets through the DoD Clearance Officer in the WHS Information Management Division to the ASD(NII)/DoD CIO.

5.4.3.7. Submit requests for public, internal (e.g., across DoD Components), and interagency information collection requirements to the DoD Clearance Officer in the WHS Information Management Division.

5.4.3.8. Maintain an up-to-date index of approved information collection requirements.

5.4.4. Respond only to those information collection requirements that have been symbolized; that is, assigned an information control symbol, or an OMB control number, or exempted, consistent with Reference (e).

5.4.5. Establish goals, as appropriate, consistent with critical mission needs, for reduction in the number or frequency of their internally prescribed information collection requirements.

5.4.6. Ensure that the Component assesses its information collection requirements no less frequently than every 3 years to ensure they are still valid and adequate. Actions shall be taken to accomplish modifications, cancellations, or new initiatives identified during the review. The results shall be communicated to the information requirements control activity. The DoD Component should consider the assignment of expiration dates to information collection requirements to avoid the workload burden of obtaining re-approval of their information collection requirements.

6. INFORMATION REQUIREMENTS

The Heads of the DoD Components are authorized to approve, symbolize, or exempt their own prescribed internal information collection requirements. These are collections of information that do not extend outside the Component.

7. EFFECTIVE DATE

This Instruction is effective immediately.



John G. Grimes  
Assistant Secretary of Defense for Networks  
and Information Integration/DoD Chief  
Information Officer

Enclosures - 2

- E1. References, continued
- E2. Definitions



E1. ENCLOSURE 1

REFERENCES, continued

- (e) DoD 8910.1-M, "DoD Procedures for Management of Information Requirements," June 1998
- (f) DoD 5025.1-M, "DoD Directives System Procedures," March 2003
- (g) Title 5, Code of Federal Regulations, Section 1320
- (h) DoD Directive 5400.11, "Department of Defense Privacy Program," November 16, 2004
- (i) DoD Directive 5400.7, "DoD Freedom of Information Act (FOIA) Program," October 28, 2005
- (j) ASD(NII)/DoD CIO Privacy Impact Assessment (PIA) Guidance, October 28, 2005<sup>1</sup>
- (k) DoD Instruction 1100.13, "Surveys of Department of Defense Personnel," November 21, 1996
- (l) Section 1782 of title 10, United States Code
- (m) Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," November 28, 2000<sup>2</sup>
- (n) DoD Directive 3216.2, "Protection of Human Subjects and Adherence to Ethical Standards in DoD-Supported Research", March 25, 2002

---

<sup>1</sup> This document is available at the following Web site: <http://www.dod.mil/cio-nii/cio/pia.shtml>.

<sup>2</sup> This document is available at the following Web site:  
<http://clinton4.nara.gov/OMB/circulars/a130/a130trans4.html>.

## E2. ENCLOSURE 2

### DEFINITIONS

E2.1. Burden. The total time, effort, or financial resources expended for:

E2.1.1. Reviewing instructions.

E2.1.2. Acquiring, installing, and utilizing technology and systems.

E2.1.3. Adjusting the existing ways to comply with any previously applicable instructions and requirements.

E2.1.4. Searching data sources.

E2.1.5. Completing and reviewing the collection of information.

E2.1.6. Transmitting, or otherwise disclosing the information.

E2.2. Collection of Information. Obtaining or causing to be obtained, soliciting, or requiring of facts or opinions regardless of form/format used.

E2.3. DoD Component Internal Information Requirements. DoD Component internal information requirements are those information requirements that are internal to a particular DoD Component and approved by that Component. Examples of these would be OSD internal, Army internal, Air Force internal, Navy internal, DLA internal, etc.

E2.4. DoD Internal Information Requirements. DoD internal information requirements are those information requirements that require the collection of information from two or more DoD Components and require approval by the DoD Internal Reports Manager, who resides in WHS. Examples of these would be if a survey draws subjects from two or more Military Services, or if a survey draws subjects from a Military Service and another OSD Component.

E2.5. Information. Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numeric, graphic, cartographic, narrative, or audiovisual forms. (See Reference (m))

E2.6. Information Collection Budget. An annual comprehensive budget of burden hours for all collections of information from the public to be conducted or sponsored by a Federal Agency in the succeeding 12 months.

E2.7. Information Requirements Assessment. The analysis of ongoing information requirements to ascertain the need for the information, the cycle of reporting, the timeliness of the requirement, the accuracy of the information, and the cost-effectiveness of the requirement.

E2.8. Interagency Information Collection Requirement. Any requirement that involves collecting information from or providing information to a Federal Agency from one or more other Federal Agencies. Interagency information collection requirements, where the Department of Defense is the requesting agency, are approved through the DoD internal information requirements process.

E2.9. Privacy Impact Assessment (PIA). The analysis of how information is handled:

E2.9.1. To ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy.

E2.9.2. To determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system.

E2.9.3. To examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

E2.10. Sponsor. A sponsoring agency is one that causes another agency to collect information, contracts or enters into a cooperative agreement with a person to collect information, or requires a person to provide information to another person, or otherwise causes another person to obtain, retain, solicit, or require the disclosure to third parties or the public of information by or for an agency.

E2.11. Surveys of Persons. Systematic data collections, using personal or telephonic interviews, or self-administered questionnaires paper or Web-based from a sample of 10 or more persons as individuals or representatives of agencies that elicit attitudes, opinions, behavior, and related demographic, social, and economic data to identical questions that are to be used for statistical compilations for research and/or policy assessment purposes.

**Attachment 6**  
**Military OneSource Program**  
**Government Furnished Information (GFI)**  
**Government Furnished Property (GFP)**

**Military OneSource Logo**

**Military OneSource Phone Number: 800-342-9647**

**Military OneSource Collect Call Number: 484-530-5908**

**TTY/TDD Number: 866-607-6794**

**Spanish Line: 877-888-0727**

800-375-5971 - Army Spanish

877-989-5392 - Navy Spanish

**Military OneSource URLs:**

[www.militaryonesource.com](http://www.militaryonesource.com)

[www.armyonesource.com](http://www.armyonesource.com)

[www.mccsonesource.com](http://www.mccsonesource.com)

[www.navyonesource.com](http://www.navyonesource.com)

[www.airforceonesource.com](http://www.airforceonesource.com)

**Military Severely Injured URLs:**

[www.militaryseverelyinjured.com](http://www.militaryseverelyinjured.com)

[www.militaryseverelyinjured.org](http://www.militaryseverelyinjured.org)

[www.militaryseverelyinjured.net](http://www.militaryseverelyinjured.net)

**Joint Family Resource Center URLs:**

[www.JFSAP.com](http://www.JFSAP.com)

[www.JFSAP.org](http://www.JFSAP.org)

[www.JFSAP.net](http://www.JFSAP.net)

**Spouse Education and Career Opportunities:**

MyCAA Portal at <https://aiportal.acc.af.mil/map>.

**Attachment 6**  
**Military OneSource Program**  
**Government Furnished Information (GFI)**  
**Government Furnished Property (GFP)**

**Wounded Warrior Resource Tracking System**

High Level Specs are as follows:

Operating System: Red Hat Linux v4.x

Database: Oracle 10gR2 (10.2.0.3)

Built using COTS Software: Oracle Application Express version 3.x

(Oracle Application Express is a rapid Web application development tool for the Oracle database. Using only a Web browser and limited programming experience, you can develop professional applications that are both fast and secure.)

**The following materials will be available to transfer:**

Reference attached Fulfillment Materials List (Attachment 6A).

## Military OneSource Fulfillment Materials List

Item Description	Type	Quantity	Cartons	Skids	Received into Stock
<b>Casualty</b>					
MILITARY WIDOW BOOK	BOOK	1000	28	1	
SURVIVOR FACT SHEET	SHEET	1000	1	1	
THE DAYS AHEAD ENGLISH BINDER	MATERIAL	1000	167	6	
THE DAYS AHEAD SPANISH BINDER	MATERIAL	500	84	3	
<b>Child and Youth</b>					
BULLIES ARE A PAIN IN THE BRAIN	BOOK	2000	21	1	
HOB&T PARENT'S DEATH BOOK	BOOKLET	100,000	250	8	
HOB&T PARENT'S DEPLOYMENT, INJURY, DEATH	BOOKLET	100,000	250	8	
HOME AGAIN BOOK	BOOK	10,000	250	6	
I'M HERE FOR YOU NOW BOOK	BOOK	10,000	209	8	
MC&FP BIRTH TO FIVE BOOK SET	BOOKS	115	115	4	
MC&FP INFANT BOOK SET	BOOKS	115	115	4	
MEMORY BOX COMFORT KIT	MATERIAL	3,750	375	21	
OVER THERE MOMMY BOOK	BOOK	10,000	250	8	
OVER THERE CD	CD	20,000	50	2	
OVER THERE DADDY BOOK	BOOK	10,000	250	8	
PRESCHOOL BOOK LIST	BOOKS	115	115	4	
SESAME STREET "WHEN FAMILIES GRIEVE DVD"	DVD	200,000	4000	125	
SESAME STREET DVD TALK LISTEN CONNECT	DVD	250,000	5000	156	
TAKING THE "DUH" OUT OF DIVORCE	BOOK	1000	9	1	

## Military OneSource Fulfillment Materials List

Item Description	Type	Quantity	Cartons	Skids	Received into Stock
TODDLER BOOK LIST	BOOKS	115	115	4	
TRUE OR FALSE? TESTS STINK?	BOOK	1,000	9	1	
WHAT ON EARTH DO YOU DO WHEN SOMEONE DIE	BOOK	1,000	8	1	
WITH YOU ALL THE WAY KIT	MATERIAL	3,750	625	35	
<b>Defense Center of Excellence</b>					
FRIENDS & FAMILY OF SERVICE MEMBERS	GUIDEBOOK	20,000	800	25	
<b>Department of Defense Education Activity</b>					
DODEA SPECIAL EDUCATION TRAINING MODULES	MATERIAL	1500	32	1	
STUDENTS AT THE CENTER BOOKLET	BOOKLET	10,000	250	8	
STUDENTS AT THE CENTER DVD	DVD	10,000	200	7	
<b>Financial</b>					
FTC #S TO KNOW & PLACES TO GO BOOKMARKS	BOOKMARK	50,000	8	1	
10 EASY WAYS TO SAVE FLYER	FLYER	100,000	50	2	
FTC BUILDING A BETTER CREDIT REPORT BOOK	BOOK	5,000	25	1	
FDIC CONSUMER NEWS CARDS	CARD	5,000	3	1	
COUPON ORGANIZER AND FLYER	MATERIAL	25,000	417	14	
DOLLAR SIGN PEN	MATERIAL	250,000	278	9	
FINANCIAL COUNSELING FLYER	FLYER	100,000	50	2	
FINANCIAL FITNESS VIZ KIT	MATERIAL	50,000	1,852	58	
FDIC FORECLOSURE RESCUE LOAN BROCHURES	BROCHURE	5,000	9	1	
HAVE YOU FED YOUR PIG BOOKMARKS	BOOKMARK	50,000	8	1	

## Military OneSource Fulfillment Materials List

Item Description	Type	Quantity	Cartons	Skids	Received into Stock
HAVE YOU FED YOUR PIG RACK CARD	RACK CARD	50,000	12	1	
HAVE YOU FED YOUR PIG TODAY MAGNET	MATERIAL	50,000	50	2	
HAVE YOU FED YOUR PIG WALLET CARD	WALLET CARD	200,000	40	2	
MANAGING YOUR ACCOUNT BOOKLET	BOOKLET	10,000	200	7	
FTC MILITARY ID THEFT TRIFOLD BROCHURE	BROCHURE	50,000	34	2	
FDIC MONEY SMART CBI CARDS	POST CARD	10,000	2	1	
MOSKITF(TAKE CHARGE POCKET FOLD)	MATERIAL	250,000	1,112	35	
NASAA'S CUTTING THROUGH CONFUSION BROCHURE	BROCHURE	10,000	7	1	
SAVE AND INVEST FOLDER(FRA1055)	MATERIAL	25,000	1,924	61	
FTC SENTINEL/MILITARY BOOKMARK	BOOKMARK	50,000	8	1	
SUMRY OF THE TRIFT SVINGS PLN BK T	BOOKLET	10,000	5	1	
TAX CUT FLYER	FLYER	50,000	25	1	
TSP WEBSITE LEAFLET	LEAFLET	10,000	2	1	
<b>Madigan Army Medical Center</b>					
MILITARY YOUTH COPING WITH SEPARATION	DVD	15,000	188	6	
MR. POE & FRIENDS DISCUSS FAMILY REUNION	DVD	15,000	188	6	
<b>Military OneSource</b>					
CHILL DRILL PLAYAWAY	MATERIAL	30,000	250	8	
COMBAT SLEEP CARD	MATERIAL	50,000	160	5	
COMING HOME BOOKLET	BOOKLET	150,000	462	15	
DEPLOYMENT RESOURCES FLYER	FLYER	150,000	75	2	



## Military OneSource Fulfillment Materials List

Item Description	Type	Quantity	Cartons	Skids	Received into Stock
MIITARY ONESOURCE GIFT BAGS	MATERIAL	20,000	80	3	
MILITARY MAGNETS (OVER SEAS)	MATERIAL	650,000	542	17	
MILITARY MOS BROCHURE	BROCHURE	500,000	334	11	
MILITARY ONESOURCE (SPANISH) BI-FOLD 4X8	MATERIAL	25,000	17	1	
MOS SCRATCH PADS	MATERIAL	400,000	1,852	68	
MOS BANNER	MATERIAL	100	10	1	
MOS BELT CLIP	MATERIAL	100,000	100	4	
MOS BOOKMARKS	BOOKMARKS	50,000	8	1	
MOS CARABINERS	MATERIAL	50,000	277	9	
MOS COUNSELING BROCHURE	BROCHURE	400,000	200	7	
MOS EUROPE BANNER (00-800#)	MATERIAL	100	10	1	
MOS GENERIC RACK CARD	RACK CARD	150,000	46	2	
MOS HEALTH LIBRARY FLYER	FLYER	100,000	50	2	
MOS LANYARD	MATERIAL	300,000	600	19	
MOS MOUSEPAD	MATERIAL	150,000	1,200	38	
MOS PACIFIC BANNERS (*800)	MATERIAL	100	10	1	
MOS PENS	MATERIAL	250,000	278	9	
MOS STATESIDE WALLET CARD	WALLET CARD	700,000	140	5	
MOS WATER BOTTLE	MATERIAL	10,000	200	7	
NEW RECRUIT CARD	MATERIAL	50,000	277	9	
OUTREACH FOLDER	MATERIAL	200,000	160	5	

## Military OneSource Fulfillment Materials List

Item Description	Type	Quantity	Cartons	Skids	Received into Stock
PROMOTIONAL TOOLS FLYER	FLYER	50,000	25	1	
STSF-T EUCOM FLYER	FLYER	30,000	15	1	
WHAT CAN MOS DO FOR YOU FLYER?(ENG VERSI	FLYER	200,000	100	4	
WALLET CARDS	MATERIAL	10,000	1	N/A	
WHAT CAN MOS DO FOR YOU FLYER?(SP VERSIO	FLYER	50,000	25	1	
<b>Morale, Welfare, and Relief</b>					
MOS ON-LINE LIBRARY RESOURCE FLYER	FLYER	100,000	50	2	
ON-LINE LIBRARY RACK CARD	RACK CARD	25,000	16	1	
<b>Spouse Education and Career Office</b>					
MOS WHAT SUITS YOU RACK CARD	RACK CARD	50,000	32	2	
<b>Special Needs</b>					
DOD SCOR-SP ADULT KIT	MATERIAL	2500	167	6	
DOD SCOR-SP CARE ORG KIT/CD	MATERIAL	5000	333	11	
EFMP SPECIAL NEEDS FLYER	FLYER	100,000	50	2	
SPEC NEEDS PARENT TOOL KIT	MATERIAL	5,040	90	2	
<b>Wounded Warrior Resource Center</b>					
KEEPING IT ALL TOGETHER BINDER	MATERIAL	2,500	500	16	
MOS JFSAP RACK CARD	RACK CARD	150,000	46	2	
WWRC FLYER	FLYER	50,000	25	1	
WWRC LANYARD	MATERIAL	100,000	200	7	
WWRC WALLET CARD	WALLET CARD	200,000	40	2	

**Attachment 7**  
**Military OneSource Program**  
**Quality Assurance Surveillance Plan (QASP)**

## **INTRODUCTION**

The role of the government in quality assurance is to ensure contract standards are achieved. The purpose of the QASP is to identify the methods and procedures the Government will use to evaluate contractor actions while performing the requirements in the Performance Work Statement (PWS). It is designed to provide an effective surveillance method by monitoring contractor performance for each listed performance objective in the Performance Requirements Summary Military OneSource contract.

The QASP provides a systematic method to evaluate the services the contractor is required to furnish. It is essential that the Government directs and oversees the maintenance as a quality standard for the Military OneSource Program to ensure superior services are provided to service members and their families.

## **PERFORMANCE REQUIREMENTS SUMMARY (PRS)**

*Overview.* This PRS identifies critical success factors for the contract. It identifies both the performance objectives for those factors and the performance threshold required for each performance objective. The Government reserves the right to monitor all services called for in the contract to determine whether or not the performance objectives and goals were met.

The absence of any contract requirement from the PRS shall not detract from its enforceability nor limit the rights or remedies of the Government under any other provision of the contract.

*Performance Remediation.* Performance of services will be evaluated to determine whether it met the performance threshold. Re-performance is the preferred method of correcting any unacceptable performance. The contractor shall provide the Government a written response explaining why the performance threshold was not met, how performance will be returned to acceptable levels, and how recurrence will be prevented in the future.

*Performance Requirements Summary*

## Call Center Metrics

<b>Performance Requirement (PR)</b>	<b>Standard</b>	<b>Surveillance</b>
<b>1.1 Provide responsive service to callers</b>	Calls answered live within 20 seconds of first ring; 90%	Contractor monthly reports, government sampling
<b>1.2 Provide responsive service to callers</b>	Abandon rate <.5%	Contractor monthly reports, government sampling
<b>1.3 Provide responsive service to callers</b>	Messages taken < .5% of calls	Contractor monthly reports, government sampling
<b>1.4 Provide responsive service to callers</b>	Hold time during triage <5 minutes; 95%	Contractor monthly reports, government sampling
<b>1.5 Provide responsive service to callers</b>	Callbacks completed within 48 hours; 95%	Contractor monthly reports, government sampling
<b>1.6 Provide translation services service to callers</b>	Availability of services; 100%	Contractor monthly reports, government sampling

## Case Metrics

<b>Performance Requirement (PR)</b>	<b>Standard</b>	<b>Surveillance</b>
<b>Follow Up Attempts</b>	100% as agreed to by caller and as clinically appropriate	Contractor monthly reports, government sampling
<b>Service Breakdowns** as a Percentage of Cases</b>	< .5%	Contractor monthly reports, government sampling
<b>Document Translations</b>	Completed within 3 business days; 95%	Contractor monthly reports, government sampling

\*\* Client complaints substantiated by quality team.

## User Satisfaction Metrics

<b>Performance Requirement (PR)</b>	<b>Standard</b>	<b>Surveillance</b>
<b>% of Participants Surveyed</b>	100% of those appropriate for survey	Contractor monthly reports, government sampling
<b>% Overall Satisfaction</b>	95%	Contractor monthly reports, government sampling
<b>% Satisfied with Educational Materials (received in a timely manner, readability, utility &amp; validity)</b>	95%	Contractor monthly reports, government sampling

<b>User Satisfaction with translation/ interpretation services</b>	95%	Contractor monthly reports, government sampling
<b>User Satisfaction with nonmedical counseling</b>	92%	Contractor monthly reports, government sampling
<b>User Satisfaction with nonmedical financial counseling</b>	92%	Contractor monthly reports, government sampling
<b>User Satisfaction with nonmedical health and wellness coaching</b>	92%	Contractor monthly reports, government sampling
<b>User Satisfaction with face to face experience in relation to nonmedical counseling</b>	92%	Contractor monthly reports, government sampling
<b>User Satisfaction with telephonic experience in relation to nonmedical counseling</b>	92%	Contractor monthly reports, government sampling
<b>User Satisfaction with web-based experience in relation to nonmedical counseling</b>	92%	Contractor monthly reports, government sampling

#### Educational Materials

<b>Performance Requirement (PR)</b>	<b>Standard</b>	<b>Surveillance</b>
<b>Educational and Informational Materials produced in a timely manner</b>	Produced within timeline mutually agreed by contractor and customer; 100%	Contractor monthly reports, government sampling
<b>Educational Materials and Referrals Shipped in a timely manner</b>	Shipped within 48 hours; 98%	Contractor monthly reports, government sampling

#### Employee Quality/Training Metrics

<b>Performance Requirement (PR)</b>	<b>Standard</b>	<b>Surveillance</b>
-------------------------------------	-----------------	---------------------

<b>Employee Training</b>	Contractor Provides 100% of Orientation Training Within 30 days of hire	Contractor monthly reports, government sampling
<b>Employee refresher training</b>	Annually	Contractor monthly reports, government sampling

## Case Management Metrics

<b>Performance Requirement (PR)</b>	<b>Standard</b>	<b>Surveillance</b>

CMS uptime, excluding scheduled maintenance

99%

CMS scheduled maintenance

&lt;= 1 hr per month; 90%

## Reporting Metrics

<b>Performance Requirement (PR)</b>	<b>Standard</b>	<b>Surveillance</b>
<b>Monthly report timeliness</b>	95% Delivered by 10 <sup>th</sup> of each month	Government receipt of reports
<b>Annual report timeliness</b>	100% Delivered 60 days after end of POP	Government receipt of reports

## Provider Network Metrics

<b>Performance Requirement (PR)</b>	<b>Standard</b>	<b>Surveillance</b>
<b>Provider availability</b>	92% within 30 miles or 15 minutes of client	Contractor monthly reports, government sampling
<b>Network training</b>	100% within 30 days if hire	Contractor monthly reports, government sampling
<b>Network Refresher training</b>	100% annually	Contractor monthly reports, government sampling

## Non-Medical Counseling

<b>Performance Requirement (PR)</b>	<b>Standard</b>	<b>Surveillance</b>
<b>Clinical Quality* of STSF cases (as measured through clinical supervision)</b>	95%	
<b>Urgent STSF cases</b>	92% within 1 business day	

<b>scheduled for face to face appointment</b>		
<b>Non-urgent STSF cases scheduled for face to face appointment</b>	92% within 3 business days	
<b>Case information posted to CMS</b>	95%	
<b>Service breakdowns** as a percentage of cases</b>	< .5%	Contractor monthly reports, government sampling

\* Contractor shall provide written definition and parameters for Clinical Quality of Cases

\*\* Client complaints substantiated by quality team.

### Financial Counseling

<b>Performance Requirement (PR)</b>	<b>Standard</b>	<b>Surveillance</b>
<b>Quality* of financial cases (as measured through clinical supervision)</b>	95%	Contractor monthly reports, government sampling
<b>Urgent financial cases scheduled for appointment</b>	92 % within 1 business day	Contractor monthly reports, government sampling
<b>Non-urgent financial cases scheduled for appointment</b>	92% within 3 business days	Contractor monthly reports, government sampling
<b>Case information posted to CMS</b>	95% within 3 business days of receipt	
<b>Case information is furnished to provider of services</b>	100% prior to scheduled appointment and/or within 3 business days	Contractor monthly reports, government sampling
<b>Service breakdowns** as a percentage of cases</b>	< .5%	Contractor monthly reports, government sampling

\*Contractor shall provide written definition and parameters for Quality of financial cases

\*\* Client complaints substantiated by quality team.

### Health and Wellness Coaching

<b>Performance Requirement (PR)</b>	<b>Standard</b>	<b>Surveillance</b>
<b>Quality* of health and wellness cases (as measured through clinical supervision)</b>	Consistent with COA standards of review; 95%	Contractor monthly reports, government sampling
<b>Urgent health and wellness cases scheduled for appointment</b>	92% within 1 business day	Contractor monthly reports, government sampling

<b>Non-urgent health and wellness cases scheduled for appointment</b>	92% within 3 business days	Contractor monthly reports, government sampling
<b>Case information posted</b>	95% within 3 business days	Contractor monthly reports, government sampling
<b>Case information is furnished to provider of services</b>	100% prior to scheduled appointment and/or within 3 business days	Contractor monthly reports, government sampling
<b>Service breakdowns** as a percentage of cases</b>	< .5%	Contractor monthly reports, government sampling
<b>Case information transferred to 1-800/website contractor</b>	95% within 3 business days of case closure	Contractor monthly reports, government sampling

\*Contractor shall provide written definition and parameters for Quality of health and wellness cases

\*\* Client complaints substantiated by quality team.

#### Wounded Warrior Metrics

<b>Performance Requirement (PR)</b>	<b>Standard</b>	<b>Surveillance</b>
<b>Cases resolved within 96 hours</b>	100%	

#### Joint Family Support Assistance Program Metrics

<b>Performance Requirement (PR)</b>	<b>Standard</b>	<b>Surveillance</b>
N/A		

#### Spouse Education & Career Opportunities Metrics

<b>Performance Requirement (PR)</b>	<b>Standard</b>	<b>Surveillance</b>
N/A		



**Attachment 8**  
**Military OneSource Program**  
**Acronyms / Symbols**

The following are examples of acronyms that may appear in this contract:

ACA	Associate Contractor Agreement	N/A	Not Applicable
ACRN	Accounting Classification Reference Number	NSP	Not Separately Priced
		NTE	Not To Exceed
AMT	Amount	OCONUS	Outside Continental United States
ASR	As Required		
CLIN	Contract Line Item Number	ODBC	Open Database Connectivity
CONUS	Continental United States	OEF	Operation Enduring Freedom
COR	Contracting Officer Representative	OIF	Operation Iraqi Freedom
DoD	Department of Defense	CO	Contracting Officer
EA	Each	POC	Point of Contact
EST	Estimated	PWS	Performance Work Statement
FFP	Firm Fixed Price	QASP	Quality Assurance Surveillance Plan
FY	Fiscal Year		
GWOT	Global War on Terrorism	QOL	Quality of Life
GFI	Government Furnished Information	QTY	Quantity
		SLIN	Sub Line Item Number
IPR	In-Process Review	SLE	Service Level Expert
LO	Lot	SOP	Standard Operating Procedures
MC&FP	Military Community and Family Policy	SOW	Statement of Work
MO	Month	TBD	To be Determined
		TBF	To be Funded
		T&M	Time and Material

**Attachment 10**  
**Military OneSource Program**  
**Languages**

**Tier one:**

Spanish, French, Italian, German, Russian, and Portuguese

**Tier two:**

Arabic, Bulgarian, Chinese Mandarin, Czech, Danish, Dutch, Estonian, Finish, Greek, Georgian ,  
Hindu, Hebrew, Hungarian, Indonesian, Japanese, Korean, Latvian, Lithuanian, Norwegian,  
Polish, Romanian, Serbian, Slovak, Swedish, Tagalog, Thai, Turkish, Vietnamese, Ukrainian,  
Uzbek

**Tier three:**

Albanian, Cantonese, Creole, Farsi, Flemish, Islandic, Karakalpak, Khmer, Lao, Malayan,  
Mongolian, Swahili, Tajik, Tatar, Telugu, Tibetan and all other languages

**ATTACHMENT - 11**  
**PERFORMANCE WORK STATEMENT (PWS)**  
**MANDATORY COMPLIANCE REQUIREMENTS**  
**MILITARY ONESOURCE PROGRAM**

- 1. REFERENCES.** The following specified documents are requirements of this PWS. Nothing in these documents, however, supersedes applicable laws and regulations unless a specific exemption has been obtained. The references below intend to reflect the current revision, change, or update to each document.

**1.1. Department of Defense Directives.**

- 1.1.1.** DoDD 8500.01E Information Assurance (IA) ASD(NII)/DoD CIO  
(Available at <http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf>)
- 1.1.2.** DoDD 8570.01 Information Assurance Training, Certification, and Workforce Management ASD(NII)/DoD CIO 15 August 2004  
(Available at <http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf>)
- 1.1.3.** DoDD 5230.9, Clearance of DoD Information for Public Release
- 1.1.4.** DoDD 5230.25 Withholding of Unclassified Technical Data from Public Disclosure  
(Available at [http://jitc.fhu.disa.mil/jitc\\_dri/pdfs/d523025p.pdf](http://jitc.fhu.disa.mil/jitc_dri/pdfs/d523025p.pdf))
- 1.1.5.** DoDD 5200.2, "DoD Personnel Security Program" April 9, 1999
- 1.1.6.** DoD 5500.7-R, Joint Ethics Regulation (JER), Change 6 Incorporated,  
:<http://www.dtic.mil/whs/directives/corres/html/55007r.htm>
- 1.1.7.** DoD 5400.11-R, "Department of Defense Privacy Program", May 8, 2007 (*Incorporating Change 1, September 1, 2011*);  
<http://www.dtic.mil/whs/directives/corres/pdf/540011r.pdf>
- 1.1.8.** DoDD O-8530.1, "Computer Network Defense (CND)", January 8, 2001
- 1.1.9.** DoDD 8910.1, "Management and Control of Information Requirements"

**1.2. Department of Defense Instructions**

- 1.2.1.** DoDI 6400.06, "Domestic Abuse Involving DoD Military and Certain Affiliated Personnel," August 21, 2007 (*Incorporating Change 1, September 20, 2011*)
- 1.2.2.** DoDI 6490.06, "Counseling Services for DoD Military, Guard and Reserve, Certain Affiliated Personnel, and Their Family Members," April 2009 (*Incorporating Change 1, July 21, 2011*)  
(Available at <http://www.dtic.mil/whs/directives/corres/pdf/649006p.pdf>)
- 1.2.3.** DoDI 6495.02 "Sexual Assault Prevention and Response (SAPR) Program," June 23, 2006
- 1.2.4.** DoDI 8500.2 Information Assurance Implementation  
(Available at <http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf>)
- 1.2.5.** DoDI 8510. DoD Information Assurance Certification and Accreditation Process (DIACAP)  
(Available at: <http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf>)  
<http://iase.disa.mil/diacap/>
- 1.2.6.** DoDI 8570.01-M Information Assurance Workforce Improvement Program  
(*Incorporating Change 3, January 24, 2012*)  
(Available at: <http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf>)
- 1.2.7.** DoDI 5400.7-R DoD Freedom of Information Act Program
- 1.2.8.** DoDI 8910.01, Information Collection and Reporting, March 6, 2007
- 1.2.9.** DoDI 3001.02, May 3, 2010, Personnel Accountability in Conjunction With Natural or Manmade Disasters.  
[www.dtic.mil/whs/directives/corres/pdf/300102p.pdf](http://www.dtic.mil/whs/directives/corres/pdf/300102p.pdf)

**ATTACHMENT - 11**  
**PERFORMANCE WORK STATEMENT (PWS)**  
**MANDATORY COMPLIANCE REQUIREMENTS**  
**MILITARY ONESOURCE PROGRAM**

- 1.2.10.** DoDI 1342.27, "Personal Financial Management for Service Members," November 12, 2004

**1.3. OMB Memos and Circulars**

- 1.3.1.** OMB M-10-22 Guidance for Online Use of Web Measurement and Customization Technologies
- 1.3.2.** OMB M-05-04 Policies for Federal Agency Public Websites, December 17, 2004
- 1.3.3.** OMB M-10-23 Guidance for Agency Use of Third-Party Websites and Applications, June 25, 2010
- 1.3.4.** OMB M-06-15 Safeguarding Personally Identifiable Information, May 22, 2006
- 1.3.5.** OMB Circular A-130, "Management of Federal Information Resources, Transmittal 4," November 30, 2000
- 1.3.6.** FPC 65, Federal Executive Branch Continuity of Operations (COOP)  
[http://www.fema.gov/pdf/library/fpc65\\_0604.pdf](http://www.fema.gov/pdf/library/fpc65_0604.pdf)

**1.4. Public Law**

- 1.4.1.** Public Law 105-277-OCT. 21, 1998 Children's Online Protection Act of 1998
- 1.4.2.** Public Law 100-235 Computer Security Act of 1987
- 1.4.3.** Public Law 107-347 E-Government Act of 2002
- 1.4.4.** Public Law 104-13-MAY 22, 1995 Paperwork Reduction Act
- 1.4.5.** Public Law 105-220, Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998  
<http://www.section508.gov/>

**1.5. U.S. Code.**

- 1.5.1.** Section 2224 of title 10, United States Code, "Defense Information Assurance Program"
- 1.5.2.** Sections 1423 and 1451 of title 40, United States Code, "Division E of the Clinger-Cohen Act of 1996"
- 1.5.3.** Section 278g-3 of title 15, United States Code, "Computer Security Act of 1987"
- 1.5.4.** Section 552 of title 5, United States Code, "Freedom of Information Act"  
<http://www.justice.gov/opcl/privstat.htm>
- 1.5.5.** Section 3101 of Title 44, United States Code, "Records Management by Federal Agencies"

**1.6. DEFENSE INFORMATION SYSTEMS AGENCY STIG GUIDANCE,**  
<http://iase.disa.mil/stigs/stig/index.html>

- 1.6.1.** DOD DISA Database Security Technical Implementation Guide (STIG)
- 1.6.2.** DoD DISA Application Security And Development Security Technical Implementation Guide (STIG)
- 1.6.3.** DoD DISA Enclave Security Technical Implementation Guide (STIG)

**Attachment 12**  
**Military OneSource Program**  
**Position Description**

**JOINT FAMILY SUPPORT AND ASSISTANCE PROGRAM**  
**MILITARY ONESOURCE CONSULTANTS**

**Job Description:**

A Military OneSource (MOS) Consultant will be located at each Joint Family Support Assistance Program (JFSAP) location and become a state/regional expert on the resources available in the communities where Service members and their families reside, including information on benefits, etc.

The JFSAP MOS Consultant, working collaboratively with other JFSAP MOS Consultants will create a “high-tech, high touch” web-enabled united community to connect military families with each other and with supportive resources 24/7. The JFSAP staff will travel throughout the state as appropriate to meet with families and unit family support staff to assess needs, form relationships with community resources, and provide or refer to services via a warm "hand-off."

JFSAP staff will partner with and augment activities of Service Family Centers, Guard and Reserve programs (including Inter-Service Family Assistance Committees (ISFACs), unit family support staff officers, and other programs and services to build coalitions and connect Federal, state, and local resources and non-profit organizations to support Active Duty, Guard and Reserve families to:

- Identify family needs;
- Catalogue existing family programs and supportive resources; determine how well those efforts are meeting family needs;
- Identify problems and/or gaps in service/resources;
- Determine methods to fill the gaps and enhance existing support systems' efforts; and
- Plan and implement a comprehensive, integrated, mobile service delivery system.

**Major Responsibilities:**

***As a member of the JFSAP team:***

- Build coalitions, coordinate with and connect Federal, state, and local resources and non-profit organizations to support Active Duty, Guard and Reserve families; Coordinate and plan service delivery under direction of the National Guard Joint Force Headquarters Command (JFHQ) J-1 and the State Family Program Director (SFPD).
- Financial and Material Assistance
  - The JFSAP MOS Program Manager will connect families with trained financial counselors who will provide personal and family financial management education, information services, counseling, and assistance to assist Service members and families with personal financial readiness, credit and budget counseling.
- Increase availability of resources for family members

- Increase awareness of Active Duty/Guard/Reserve members and families to existing family assistance services and resources, including MOS resources
- Inform leadership and service providers about the range of available programs and services, and how they may be accessed
- Integrate services and programs into a comprehensive delivery system that responds to the needs of members and families at all stages of the deployment cycle and provides:
  - Information & Referral
  - Financial & Material Assistance
- Serve as regional expert on resources available in communities where members and families reside
- Explore discounts for military families with community organizations and businesses
- Coordinate financial counseling for families
- Partner with groups, e.g. the ISFAC, to integrate military and civilian resources
- Identify, catalog (hard copy and electronic) and market resources available to members and families;
- Prepare hard-copy and electronic matrices and marketing materials that describe resource(s); what they have to offer; to whom; how to access; and contact person(s)
- Work with MOS to build child care capability and provide resource and referral to meet the child care needs for full-day, part-day and respite care.
  - Assess child care needs of families
  - Explore funding sources to “buy down” the cost of childcare
  - Expand partnerships to bridge the gap between need and current program delivery
  - Explore new partnerships
  - Expand weekend, respite, and short-term programs and services
  - Provide information about on-base MWR resources (fitness, sports and recreation; entertainment; lodging; exchange and commissaries); provide the same information about off-base community resources including those that offer discounts to military families.

***Establish and maintain relationships with customer contacts:***

- Establish working relationships with key contacts within your assigned region/state.
- Maintain POC information for each region and site (installation, base, etc), including but not limited to: name, rank/title, phone, fax, e-mail, mailing address.
- Identify databases and information that needs to be developed to meet needs at the state and/or regional level, help identify and/or respond to concerns of participating states/regions and provide subject matter expertise.
- Obtain immediate information on crisis events from component or site POC to have the latest approved information for release to callers inquiring about local or national crisis response services

***Review, maintain, analyze and distribute monthly/semi-annual/annual usage report:***

- Work on enhancement of monthly report package to meet customer needs.
- Review each report package for accuracy. Resolve any issues that are noticed.
- Send monthly report to main contact and schedule time to review contents. Each month provide a summary of the monthly highlights.
- Distribute report packages to regional and local POCs. Include overall highlights and any site specific highlights that might be pertinent.

- Conduct an initial report review with every POC to be sure they understand how to read and pull information from the report.

***Act as liaison between client and service delivery:***

- Recommend ongoing enhancements to information based on feedback from state/regional Points of Contact;
- Update and expand any information based on feedback from client or information gathered during client visits, conversations, or the like;
- Gather feedback from the client on how the service is being used.

**Knowledge Skills and Abilities:**

- 4-year college degree preferred
- Prior military experience as an Active Duty, National Guard or Reserve member (or as a spouse of) preferred. Will also consider relevant civilian experience. Knowledge of armed services programs (military departments and family service type programs)
- Knowledge or experience of program marketing
- Excellent communication skills (verbal and written) including an superior ability to brief senior officers and other key constituents
- Excellent project management skills are required. 3 years project/program management experience preferred
- Must be able to act independently and be self-directed
- Must be proficient with the use of Microsoft Office products: Outlook, Word, Excel, PowerPoint
- Team player able to give and receive feedback
- Flexibility and resiliency are key traits for the successful candidate

**Working Conditions / Physical Requirements**

- Significant domestic travel required – upwards of 50%



# Department of Defense INSTRUCTION

NUMBER 1342.27  
November 12, 2004

---

---

PDUSD(P&R)

**SUBJECT:** Personal Financial Management for Service Members

References: (a) DoD Directive 1342.17, "Family Policy," December 30, 1998  
(b) DoD Directive 1344.7, "Personal Commercial Solicitation on DoD Installations," February 13, 1996  
(c) DoD Directive 1344.9, "Indebtedness of Military Personnel," October 27, 1994  
(d) DoD Instruction 1342.22, "Family Centers," December 30, 1992  
(e) through (g), see Enclosure 1

## 1. PURPOSE

This Instruction:

1.1. Implements policy, assigns responsibility, and prescribes procedures under references (a), (b), (c), and (d) for the education and training of military members in personal financial management.

1.2. Establishes a uniform approach to the education and training of Service members on personal financial management.

## 2. APPLICABILITY

This Instruction applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (referred to collectively as "DoD Components"). The term "Military Services" refers to the Army, the Navy, the Air Force, the Marine Corps, and the Coast Guard (when operating as a Service within the Department of the Navy) including their Reserve components.



### 3. DEFINITIONS

Terms used in this Instruction are defined in Enclosure 2.

### 4. POLICY

It is DoD policy that:

4.1. Service members are responsible for their personal finances. They are expected to pay their financial obligations in a proper and timely manner pursuant to Reference (c).

4.2. Service members and their families shall have access to:

4.2.1. Personal financial management programs to maintain personal readiness, to support their personal financial needs throughout their military career, and to promote their retention in the military.

4.2.2. Financial planning and counseling services to correct deficiencies that may impede personal readiness if not addressed.

4.3. To mitigate adverse impact on mission readiness, the Military Departments shall target their most aggressive education and training efforts toward junior enlisted members and families, the highest risk group for financial difficulties.

### 5. RESPONSIBILITIES

5.1. The Principal Deputy Under Secretary of Defense (Personnel and Readiness), under the Under Secretary of Defense (Personnel and Readiness), or designee, shall:

5.1.1. Establish standards for the Military Services that support member financial readiness.

5.1.2. Ensure that DoD surveys include questions that assess the personal readiness of Service members.

5.1.3. Coordinate the survey results and Military Department data with the Joint Staff.

5.2. The Under Secretary of Defense (Comptroller) is responsible for the policy governing financial education requirements for on-installation banks and credit unions in the DoD 700014-R, Volume 5, Chapter 34 (Reference (e)).

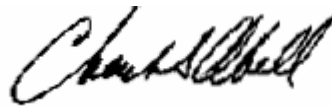
5.3. The Secretaries of Military Departments and the Heads of the DoD Components shall ensure compliance with this Instruction, by establishing procedures and allocating resources to foster Service member (and spouse) competence in personal finance to support their personal readiness; and monitor to ensure on-installation banks and credit unions comply with the financial education requirements outlined in Reference (e), paragraphs 340307(h) and 340408.

## 6. PROCEDURES

Procedures applicable to this Instruction are provided in Enclosure 3.

## 7. EFFECTIVE DATE

This Instruction is effective immediately.



Charles S. Abell  
Principal Deputy Under Secretary of Defense  
For Personnel and Readiness

Enclosures - 3

E1. References, continued

E2. Definitions

E3. Procedures for Personal Financial Management for Service Members

E1. ENCLOSURE 1  
REFERENCES, continued

- (e) DoD 7000.14-R, "Department of Defense Financial Management Regulation," Volume 5, Chapter 34, current edition
- (f) Section 1056 of title 10, United States Code
- (g) DoD Directive 5500.7, "Standards of Conduct," August 30, 1993

## E2. ENCLOSURE 2

### DEFINITIONS

E2.1.1. Basic Understanding. To comprehend the underlying principles of a subject and apply them to every day life situations.

E2.1.2. DoD Personnel. Active duty, Guard, and Reserve component members of the Military Services and civilian employees including nonappropriated fund employees and special Government employees of all offices, agencies, and departments carrying out a function on a Defense installation.

E2.1.3. Extended Absence Financial Plan. A plan developed by a Service member prior to deployment, specifying the following for the period of the absence: legal power of attorney to accomplish personal and financial requirements, a plan for meeting financial obligations, disposition of car and auto insurance, allotments by appropriate monthly expenditures, and disposition of other financial issues that might occur during the period of absence.

E2.1.4. Financial Planning and Counseling. The act of evaluating an individual's or family's income and expenditures and recommending short and long-term actions to achieve the financial goals and ensure individual, family, and mission readiness.

E2.1.5. Personal Financial Management Programs. Programs conducted by trained counselors who provide personal and family financial planning education, information services, and assistance, including but not limited to, consumer education, advice and assistance on budgeting and debt liquidation, retirement planning, and savings mid investment counseling.

E2.1.6. Personal Readiness. Service member's responsibility to prudently maintain day-to-day personal matters, and to adequately prepare for the management of personal responsibilities prior to departing on an extended absence, including: family matters and potential family contingencies, personal finances, personal property, and other personal obligations that may arise during an extended absence.

E2.1.7. Service Members. Active duty, Guard, and Reserve component members of the Military Services.

### E3. ENCLOSURE 3

#### PROCEDURES FOR PERSONAL FINANCIAL MANAGEMENT FOR SERVICE MEMBERS

E3.1.1. At a minimum, Services members shall receive assistance to accomplish the following:

E3.1.1.1. Within 3 months after arriving at the first permanent station, a Service member shall demonstrate a basic understanding of pay and entitlements, banking and allotments, checkbook management, budgeting and saving (to include the thrift savings plan), insurance, credit management, car buying, permanent change of station moves (as required by Section 1056 of title 10, United States Code, Reference (f)), and information on obtaining counseling or assistance on financial matters.

E3.1.1.2. Prior to any deployment that exceeds 4 weeks, a Military Service member shall be able to establish an extended absence financial plan as part of personal readiness preparation.

E3.1.1.3. Prior to assuming a leadership role as a supervisor, officers and noncommissioned officers shall have a basic understanding of policies and practices designed to protect junior military Service members within their command/supervisor, to include those policies and practices governing commercial solicitation as outlined in Reference (b).

E3.1.2. Instructional and informational materials shall be made available to Service members and families that assist them with critical life stages impacting personal finances (e.g., marriage, parenthood, college, and retirement).

E3.1.3. The Military Services shall provide information on personal finances to National Guard and Reserve personnel as an integral part of mobilization training.

E3.1.4. The Military Service members and their families shall be provided consumer information and assistance in handling consumer complaints.

E3.1.5. Programs shall be established to encourage spouses of Military Service members to participate in Personal Financial Management Programs.

E3.1.6. The Military Services may accept personal financial instruction and materials from organizations outside of the Department of Defense, as outlined in References (b) and (e). Preference should be extended to on-installation financial institutions to conduct financial education training and counseling as prescribed at Reference (e), paragraph 340408, as an integral part of financial service offerings, along with other on-installation personnel designated by the commander to perform this function. An instructor from an accepted source must be monitored by DoD personnel during the period of instruction.

E3.1.7. The Military Services shall respond to the request for age-appropriate classes or seminars to youth and teens as part of their school-age or youth education classes or activities at on-base Youth or Child Development facilities.

E3.1.8. The Commanders shall refer members in their commands for financial counseling and assistance by trained staff when notified of the members financial indebtedness.

E3.1.9. At a minimum one staff member within a family center shall be designated and trained to organize and execute financial planning and counseling programs for the military community. Personnel hired, contracted. or serving part time as the primary expert on personal finances for the installation or region, shall meet the following criteria:

E3.1.9.1. Possess a baccalaureate degree from an accredited college or a combination of education and experiences, which equips him or her to serve as a personal financial management counselor and maintain national certification as an Accredited Financial Counselor.

E3.1.9.2. Read and understand References (a), (b) and (c) in addition to being briefed about the pertinent provisions of DoD Directive 5500,7, "Standards of Conduct," August 30, 1993 (Reference (g)).

E3.1.9.3. Receive continuing education on personal financial management on an annual basis and maintain professional certification.



# Department of Defense INSTRUCTION

NUMBER 1344.07

March 30, 2006

---

---

USD(P&R)

SUBJECT: Personal Commercial Solicitation on DoD Installations

References: (a) DoD Directive 1344.7, "Personal Commercial Solicitation on DoD Installations," February 13, 1986 (hereby canceled)  
(b) Deputy Secretary of Defense Memorandum, "DoD Directives Review – Phase II," July 13, 2005  
(c) DoD Directive 5124.2, "Under Secretary of Defense for Personnel and Readiness (USD(P&R))," February 11, 2006  
(d) Section 577 of Public Law 109-163, "The National Defense Authorization Act For Fiscal Year 2006, January 6, 2006  
(e) through (s), see Enclosure 1

## 1. REISSUANCE AND PURPOSE

This Instruction:

1.1. Reissues Reference (a) as a DoD Instruction according to guidance in References (b) and (c).

1.2. Implements Section 577 of Public Law No. 109-163 (2006) Reference (d) and establishes policy and procedures for personal commercial solicitation on DoD installations.

1.3. Continues the established annual DoD registration requirement for the sale of insurance and securities on DoD installations overseas.

1.4. Identifies prohibited practices that may cause withdrawal of commercial solicitation privileges on DoD installations and establishes notification requirements when privileges are withdrawn.

1.5. Establishes procedures for persons solicited on DoD installations to evaluate solicitors.

1.6. Prescribes procedures for providing financial education programs to military personnel.

## 2. APPLICABILITY AND SCOPE

2.1. This Instruction applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the "DoD Components").

2.2. This Instruction does not apply to services furnished by residential service companies, such as deliveries of milk, laundry, newspapers, and related services to personal residences on the installation requested by the resident and authorized by the installation commander.

2.3. This Instruction applies to all other personal commercial solicitation on DoD Installations. It includes meetings on DoD installations of private, non-profit, tax-exempt organizations that involve commercial solicitation. Attendance at these meetings shall be voluntary and the time and place of such meetings are subject to the discretion of the installation commander or his or her designee.

## 3. DEFINITIONS

Terms used in this Instruction are defined in Enclosure 2 or in Joint Publication 1-02, "DoD Dictionary of Military and Associated Terms" (Reference (e)).

## 4. POLICY

4.1. It is DoD policy to safeguard and promote the welfare of DoD personnel as consumers by setting forth a uniform approach to the conduct of all personal commercial solicitation and sales to them by dealers and their agents. For those individuals and their companies that fail to follow this policy, the opportunity to solicit on military installations may be limited or denied as appropriate.

4.2. Command authority includes authority to approve or prohibit all commercial solicitation covered by this Instruction. Nothing in this Instruction limits an installation commander's inherent authority to deny access to vendors or to establish time and place restrictions on commercial activities at the installation.



## 5. RESPONSIBILITIES

5.1. The Principal Deputy Under Secretary of Defense for Personnel and Readiness (PDUSD(P&R)), under the Under Secretary of Defense for Personnel and Readiness, shall:

5.1.1. Identify and publish policies and procedures governing personal commercial solicitation on DoD installations consistent with the policy set forth in this Instruction.

5.1.2. Maintain and make available to installation commanders and appropriate Federal personnel the current master file of all individual agents, dealers, and companies who have their privileges withdrawn at any DoD installation.

5.1.3. Develop and maintain a list of all State Insurance Commissioners' points of contact for DoD matters and forward this list to the Military Services.

5.2. The Heads of the DoD Components shall:

5.2.1. Ensure implementation of this Instruction and compliance with its provisions.

5.2.2. Require installations under their authority to report each instance of withdrawal of commercial solicitation privileges.

5.2.3. Submit lists of all individuals and companies who have had their commercial solicitation privileges withdrawn at installations under their authority to the PDUSD(P&R) in accordance with this Instruction.

## 6. PROCEDURES

### 6.1. General

6.1.1. No person has authority to enter a DoD installation to transact personal commercial solicitation as a matter of right. Personal commercial solicitation may be permitted only if the following requirements are met:

6.1.1.1. The solicitor is duly licensed under applicable Federal, State, or municipal laws and has complied with installation regulations.

6.1.1.2. A specific appointment has been made for each meeting with the individual concerned. Each meeting is conducted only in family quarters or in other areas designated by the installation commander.

6.1.1.3. The solicitor agrees to provide each person solicited the personal commercial solicitation evaluation included in Enclosure 5 during the initial appointment. The person being solicited is not required to complete the evaluation. However, completed evaluations should be sent by the person who was solicited to the office designated by the installation commander on the back of the evaluation form.

6.1.1.4. The solicitor agrees to provide DoD personnel with a written reminder, prior to their making a financial commitment, that free legal advice is available from the Office of the Staff Judge Advocate.

6.1.2. Solicitors on overseas installations shall be required to observe, in addition to the above, the applicable laws of the host country. Upon request, the solicitor must present documentary evidence to the installation commander that the company they represent, and its agents, meet the applicable licensing requirements of the host country.

## 6.2. Life Insurance Products and Securities

6.2.1. Life insurance products and securities offered and sold to DoD personnel shall meet the prerequisites described in Enclosure 3 of this Instruction.

6.2.2. Installation commanders may permit insurers and their agents to solicit on DoD installations if the requirements of paragraph 6.1. are met and if they are licensed under the insurance laws of the State where the installation is located. Commanders will ensure the agent's license status and complaint history are checked with the appropriate State or Federal regulators before granting permission to solicit on the installation.

6.2.3. In addition, before approving insurance and financial product agents' requests for permission to solicit, commanders shall review the list of agents and companies currently barred, banned, or limited from soliciting on any or all DoD installations. This list may be viewed via the *Personal Commercial Solicitation Report* "quick link" at [www.commanderspage.com](http://www.commanderspage.com). In overseas areas, the DoD Components shall limit insurance solicitation to those insurers registered under the provisions of Enclosure 4 of this Instruction.

6.2.4. The conduct of all insurance business on DoD installations shall be by specific appointment. When establishing the appointment, insurance agents shall identify themselves to the prospective purchaser as an agent for a specific insurer.

6.2.5. Installation commanders shall designate areas where interviews by appointment may be conducted. The opportunity to conduct scheduled interviews shall be extended to all solicitors on an equitable basis. Where space and other considerations limit the number of agents using the interviewing area, the installation commander may develop and publish local policy consistent with this concept.

6.2.6. Installation commanders shall make disinterested third-party insurance counseling available to DoD personnel desiring counseling. Financial counselors shall encourage DoD personnel to seek legal assistance or other advice from a disinterested third-party before entering a contract for insurance or securities.

6.2.7. In addition to the solicitation prohibitions contained in paragraph 6.4., the DoD Components shall prohibit the following:

6.2.7.1. The use of DoD personnel representing any insurer, dealing directly or indirectly on behalf of any insurer or any recognized representative of any insurer on the installation, or as an agent or in any official or business capacity with or without compensation.

6.2.7.2. The use of an agent as a participant in any Military Service-sponsored education or orientation program.

6.2.7.3. The designation of any agent or the use by any agent of titles (for example, "Battalion Insurance Counselor," "Unit Insurance Advisor," "Servicemen's Group Life Insurance Conversion Consultant,") that in any manner, states, or implies any type of endorsement from the U.S. Government, the Armed Forces, or any State or Federal agency or government entity.

6.2.7.4. The use of desk space for interviews for other than a specific prearranged appointment. During such appointment, the agent shall not be permitted to display desk signs or other materials announcing his or her name or company affiliation.

6.2.7.5. The use of an installation "daily bulletin," marquee, newsletter, webpage, or other official notice to announce the presence of an agent and/or his or her availability.

### 6.3. Supervision of On-Base Commercial Activities

6.3.1. All pertinent installation regulations shall be posted in a place easily accessible to those conducting and receiving personal commercial solicitation on the installation.

6.3.2. The installation commander shall make available a copy of installation regulations to anyone conducting on-base commercial solicitation activities warning that failure to follow the regulations may result in the loss of solicitation privileges.

6.3.3. The installation commander, or designated representative, shall inquire into any alleged violations of this Instruction or of any questionable solicitation practices. The DD Form 2885, Personal Commercial Solicitation Evaluation, at Enclosure 5 is provided as a means to supervise solicitation activities on the installation. DD Form 2885 is available at the Department of Defense Forms Web site under DefenseLink, Publications.

6.4. Prohibited Practices. The following commercial solicitation practices shall be prohibited on all DoD installations:

6.4.1. Solicitation of recruits, trainees, and transient personnel in a group setting or "mass" audience and solicitation of any DoD personnel in a "captive" audience where attendance is not voluntary.

6.4.2. Making appointments with or soliciting military or DoD civilian personnel during their normally scheduled duty hours.

6.4.3. Soliciting in barracks, day rooms, unit areas, transient personnel housing, or other areas where the installation commander has prohibited solicitation.

6.4.4. Use of official military identification cards or DoD vehicle decals by active duty, retired, or reserve members of the Military Services to gain access to DoD installations for the purpose of soliciting. When entering the installation for the purpose of solicitation, solicitors with military identification cards and/or DoD vehicle decals must present documentation issued by the installation authorizing solicitation.

6.4.5. Procuring, attempting to procure, supplying, or attempting to supply non-public listings of DoD personnel for purposes of commercial solicitation, except for releases made in accordance with DoD Directive 5400.7 (Reference (f)).

6.4.6. Offering unfair, improper, or deceptive inducements to purchase or trade.

6.4.7. Using promotional incentives to facilitate transactions or to eliminate competition.

6.4.8. Using manipulative, deceptive, or fraudulent devices, schemes, or artifices, including misleading advertising and sales literature. All financial products, which contain insurance features, must clearly explain the insurance features of those products.

6.4.9. Using oral or written representations to suggest or give the appearance that the Department of Defense sponsors or endorses any particular company, its agents, or the goods, services, and commodities it sells.

6.4.10. DoD personnel making personal commercial solicitations or sales to DoD personnel who are junior in rank or grade, or to the family members of such personnel, except as authorized in Section 2-205 and 5-409 of the Joint Ethics Regulation, DoD 5500.7-R (Reference (g)).

6.4.11. Entering into any unauthorized or restricted area.

6.4.12. Using any portion of installation facilities, including quarters, as a showroom or store for the sale of goods or services, except as specifically authorized by DoD Directive 1330.17 and DoD Instructions 1015.10, 1000.15, and 1330.21 (References (h), (i), (j), and (k)). This does not apply to normal home enterprises that comply with applicable State and local laws and installation rules.

6.4.13. Soliciting door to door or without an appointment.

6.4.14. Unauthorized advertising of addresses or telephone numbers used in personal commercial solicitation activities conducted on the installation, or the use of official positions, titles, or organization names, for the purpose of personal commercial solicitation, except as authorized in Reference (g). Military grade and military service as part of an individual's name (e.g., Captain Smith, U.S. Marine Corps) may be used in the same manner as conventional titles, such as "Mr.", "Mrs.", or "Honorable."

6.4.15. Contacting DoD personnel by calling a government telephone, faxing to a government fax machine, or by sending e-mail to a government computer, unless a pre-existing relationship (i.e., the DoD member is a current client or requested to be contacted) exists between the parties and the DoD member has not asked for contact to be terminated.

#### 6.5. Denial, Suspension, and Withdrawal of Installation Solicitation Privileges

6.5.1. The installation commander shall deny, suspend, or withdraw permission for a company and its agents to conduct commercial activities on the base if such action is in the best interests of the command. The grounds for taking these actions may include, but are not limited to, the following:

6.5.1.1. Failure to meet the licensing and other regulatory requirements prescribed in this Instruction, or violations of the State law where the installation is located. Commanders will request that appropriate State officials determine whether a company or agent violated State law.

6.5.1.2. Commission of any of the practices prohibited in paragraphs 6.2.6 and 6.4.

6.5.1.3. Substantiated complaints and/or adverse reports regarding the quality of goods, services, and/or commodities, and the manner in which they are offered for sale.

6.5.1.4. Knowing and willful violations of Pub. L. 90-321, "Truth in Lending Act" (Reference (l)).

6.5.1.5. Personal misconduct by a company's agent or representative while on the installation.

6.5.1.6. The possession of, and any attempt to obtain supplies of direct deposit forms, or any other form or device used by Military Departments to direct a Service member's pay to a third party, or possession or use of facsimiles thereof. This includes using or assisting in using a Service member's "MyPay" account or other similar internet medium for the purpose of establishing a direct deposit for the purchase of insurance or other investment product.

6.5.1.7. Failure to incorporate and abide by the Standards of Fairness policies contained in DoD Instruction 1344.9 (Reference (m)).

6.5.2. The installation commander may determine that circumstances dictate the immediate suspension of solicitation privileges while an investigation is conducted. Upon suspending solicitation privileges, the commander shall promptly inform the agent and the company the agent represents, in writing.

6.5.3. In suspending or withdrawing solicitation privileges, the installation commander shall determine whether to limit such action to the agent alone or extend it to the company the agent represents. This decision shall be based on the circumstances of the particular case, including, but not limited to, the nature of the violations, frequency of violations, the extent to which other agents of the company have engaged in such practices, and any other matters tending to show the culpability of an individual and the company.

6.5.4. If the investigation determines an agent or company does not possess a valid license or the agent, company, or product has failed to meet other State or Federal regulatory requirements, the installation commander shall immediately notify the appropriate regulatory authorities.

6.5.5. In a withdrawal action, the commander shall allow the individual or company an opportunity to show cause as to why the action should not be taken. To "show cause" means an opportunity must be given for the aggrieved party to present facts on an informal basis for the consideration of the installation commander or the commander's designee. The installation commander shall make a final decision regarding withdrawal based upon the entire record in each case. Installation commanders shall report concerns or complaints involving the quality or suitability of financial products or concerns or complaints involving marketing methods used to sell these products to the appropriate State and Federal regulatory authorities. Also, installation commanders shall report any suspension or withdrawal of insurance or securities products solicitation privileges to the appropriate State or Federal regulatory authorities.

6.5.6. The installation commander shall inform the Military Department concerned of any denial, suspension, withdrawal, or reinstatement of an agent or company's solicitation privileges and the Military Department shall inform the Office of the PDUSD(P&R), which will maintain a list of insurance and financial product companies and agents currently barred, banned, or otherwise limited from soliciting on any or all DoD installations. This list may be viewed at [www.commanderspage.com](http://www.commanderspage.com). If warranted, the installation commander may recommend to the Military Department concerned that the action taken be extended to other DoD installations. The Military Department may extend the action to other military installations in the Military

Department. The PDUSD(P&R), following consultation with the Military Department concerned, may order the action extended to other Military Departments.

6.5.7. All suspensions or withdrawals of privileges may be permanent or for a set period of time. If for a set period, when that period expires, the individual or company may reapply for permission to solicit through the installation commander or Military Department originally imposing the restriction. The installation commander or Military Department reinstating permission to solicit shall notify the Office of the PDUSD(P&R) and appropriate State and Federal regulatory agencies when such suspensions or withdrawals are lifted.

6.5.8. The Secretaries of the Military Departments may direct the Armed Forces Disciplinary Control Boards in all geographical areas in which the grounds for withdrawal action have occurred to consider all applicable information and take action the Boards deem appropriate.

6.5.9. Nothing in this Instruction limits the authority of the installation commander or other appropriate authority from requesting or instituting other administrative and/or criminal action against any person, including those who violate the conditions and restrictions upon which installation entry is authorized.

#### 6.6. Advertising and Commercial Sponsorship

6.6.1. The Department of Defense expects voluntary observance of the highest business ethics by commercial enterprises soliciting DoD personnel through advertisements in unofficial military publications when describing goods, services, commodities, and the terms of the sale (including guarantees, warranties, and the like).

6.6.2. The advertising of credit terms shall conform to the provisions of Reference (l) as implemented by Federal Reserve Board Regulation Z according to 12 CFR Section 226 (Reference (n)).

6.6.3. Solicitors may provide commercial sponsorship to DoD Morale, Welfare and Recreation programs or events according to Reference (i). However, sponsorship may not be used as a means to obtain personal contact information for any participant at these events without written permission from the individual participant. In addition, commercial sponsors may not use sponsorship to advertise products and/or services not specifically agreed to in the sponsorship agreement.

6.6.4. The installation commander may permit organizations to display sales literature in designated locations subject to command policies. In accordance with DoD 7000.14-R, Volume 7(a) (Reference (o)), distribution of competitive literature or forms by off-base banks and/or credit unions is prohibited on installations where an authorized on-base bank and/or credit union exists.

## 6.7. Educational Programs

6.7.1. The Military Departments shall develop and disseminate information and provide educational programs for members of the Military Services on their personal financial affairs, including such subjects as insurance, Government benefits, savings, budgeting, and other financial education and assistance requirements outlined in DoD Instruction 1342.27 (Reference (p)). The Military Departments shall ensure that all instructors are qualified as appropriate for the subject matter presented. The services of representatives of authorized on-base banks and credit unions may be used for this purpose. Under no circumstances shall commercial agents, including representatives of loan, finance, insurance, or investment companies, be used for this purpose. Presentations shall only be conducted at the express request of the installation commander.

6.7.2. The Military Departments shall also make qualified personnel and facilities available for individual counseling on loans and consumer credit transactions in order to encourage thrift and financial responsibility and promote a better understanding of the wise use of credit, as prescribed in DoD 7000.14-R, Volume 5, Chapter 34 (Reference (q)).

6.7.3. The Military Departments shall encourage military members to seek advice from a legal assistance officer, the installation financial counselor, their own lawyer, or a financial counselor, before making a substantial loan or credit commitment.

6.7.4. Each Military Department shall provide advice and guidance to DoD personnel who have a complaint under Reference (m) or who allege a criminal violation of its provisions, including referral to the appropriate regulatory agency for processing of the complaint.

6.7.5. Banks and credit unions operating on DoD installations are required to provide financial counseling services as an integral part of their financial services offerings under DoD Directive 1000.11 (Reference (r)). Representatives of and materials provided by authorized banks and/or credit unions located on military installations may be used to provide the educational programs and information required by this Instruction subject to the following conditions:

6.7.5.1. If the bank or credit union operating on a DoD installation sells insurance or securities or has any affiliation with a company that sells or markets insurance or other financial products, the installation commander shall consider that company's history of complying with this Instruction before authorizing the on-base financial institution to provide financial education.

6.7.5.2. All prospective educators must agree to use appropriate disclaimers in their presentations and on their other educational materials. The disclaimers must clearly indicate that they do not endorse or favor any commercial supplier, product, or service, or promote the services of a specific financial institution.



6.7.6. Use of other non-government organizations to provide financial education programs is limited as follows:

6.7.6.1. Under no circumstances shall commercial agents, including employees or representatives of commercial loan, finance, insurance, or investment companies, be used.

6.7.6.2. The limitation in subparagraph 6.7.6.1. does not apply to educational programs and information regarding the Survivor Benefits Program and other government benefits provided by tax-exempt organizations under section (c) of 26 U.S.C. 501 (Reference (s)) or by any organization providing such a benefit under a contract with the Government.

6.7.6.3. Educators from non-government, non-commercial organizations expert in personal financial affairs and their materials may, with appropriate disclaimers, provide the educational programs and information required by this Instruction if approved by a Presidentially-appointed, Senate-confirmed civilian official of the Military Department concerned. Presentations by approved organizations shall be conducted only at the express request of the installation commander. The following criteria shall be used when considering whether to permit a non-government, non-commercial organization to present an educational program or provide materials on personal financial affairs:

6.7.6.3.1. The organization must qualify as a tax-exempt organization under section (c)(3) or 1(c)(23) of Reference (s)).

6.7.6.3.2. If the organization has any affiliation with a company that sells or markets insurance or other financial products, the approval authority shall consider that company's history of complying with this Instruction.


6.7.6.3.3. All prospective educators must use appropriate disclaimers, in their presentations and on their other educational materials, which clearly indicate that they and the Department of Defense do not endorse or favor any commercial supplier, product, or service or promote the services of a specific financial institution.

## **7. INFORMATION REQUIREMENTS**

The reporting requirements concerning the suspension or withdrawal of solicitation privileges have been assigned Report Control Symbol (RCS) DD-P&R(Q)2182 in accordance with DoD 8910.1-M (Reference (t)).

8. EFFECTIVE DATE

This Instruction is effective immediately.



**David S.C. Chu**  
**Under Secretary of Defense**  
**(Personnel and Readiness)**

Enclosures - 5

- E1. References, continued
- E2. Definitions
- E3. Life Insurance Products and Securities
- E4. The Overseas Life Insurance Registration Program
- E5. Personal Commercial Solicitation Evaluation

E1. ENCLOSURE 1

REFERENCES, continued

- (e) Joint Publication 1-02, "DoD Dictionary of Military and Associated Terms"
- (f) DoD Directive 5400.07, "Freedom of Information Act (FOIA) Program," October 28, 2005
- (g) DoD 5500.7-R, "Joint Ethics Regulation (JER)," August 30, 1993
- (h) DoD Directive 1330.17, "Military Commissaries," March 13, 1987
- (i) DoD Instruction 1015.10, "Programs for Military Morale, Welfare and Recreation (MWR)," November 3, 1995
- (j) DoD Instruction 1000.15, "Private Organizations on DoD Installations," December 20, 2005
- (k) DoD Instruction 1330.21, "Armed Services Exchange Regulations," July 14, 2005
- (l) Section 1601 of title 15, United States Code
- (m) DoD Directive 1344.9, "Indebtedness of Military Personnel," October 27, 1994
- (n) Title 12, Code of Federal Regulations, Section 226
- (o) DoD 7000.14-R, Volume 7a, Chapter 41 and 42, "DoD Financial Management Regulation," February 2002
- (p) DoD Instruction 1342.27, "Personal Financial Management for Service Members," November 12, 2004
- (q) DoD 7000.14-R, Volume 5, Chapter 34, "Procedures Governing Banks and Credit Unions and Other Financial Institutions on DoD Installation," September 2000
- (r) DoD Directive 1000.11, "Financial Institutions on DoD Installations," June 9, 2000
- (s) Section 501 of title 26, United States Code
- (t) DoD 8910.1-M, "DoD Procedures for Management of Information Requirements," June 30, 1998
- (u) Section 1751 of title 12, United States Code

## E2. ENCLOSURE 2

### DEFINITIONS

E2.1.1. Agent. An individual who receives remuneration as a salesperson or whose remuneration is dependent on volume of sales of a product or products. (Also, referred to as "commercial agent" or "producer"). In this Instruction, the term "agent" includes "general agent" unless the content clearly conveys a contrary intent.

E2.1.2. "Authorized" Bank and/or Credit Union. Bank and/or credit union selected by the installation commander through open competitive solicitation to provide exclusive on-base delivery of financial services to the installation under a written operating agreement.

E2.1.3. Banking Institution. An entity chartered by a State or the Federal Government to provide financial services.

E2.1.4. Commercial Sponsorship. The act of providing assistance, funding, goods, equipment (including fixed assets), or services to an MWR program or event by an individual, agency, association, company or corporation, or other entity (sponsor) for a specified (limited) period of time in return for public recognition or advertising promotions. Enclosure 9 of Reference (i) provides general policy governing commercial sponsorship.

E2.1.5. Credit Union. A cooperative nonprofit association, incorporated under the Credit Union Act (12 U.S.C. 1751 (Reference (u))), or similar state statute, for the purpose of encouraging thrift among its members and creating a source of credit at a fair and reasonable rate of interest.

E2.1.6. DoD Installation. For the purposes of this Instruction, any Federally owned, leased, or operated base, reservation, post, camp, building, or other facility to which DoD personnel are assigned for duty, including barracks, transient housing, and family quarters.

E2.1.7. DoD Personnel. For the purposes of this Instruction, all active duty officers (commissioned and warrant) and enlisted members of the Military Departments and all civilian employees, including nonappropriated fund employees and special Government employees, of the Department of Defense.

E2.1.8. Financial Services. Those services commonly associated with financial institutions in the United States, such as electronic banking (e.g., ATMs), in-store banking, checking, share and savings accounts, fund transfers, sale of official checks, money orders and travelers checks, loan services, safe deposit boxes, trust services, sale and redemption of U.S. Savings Bonds, and acceptance of utility payments and any other consumer-related banking services.

E2.1.9. General Agent. A person who has a legal contract to represent a company. See "Agent."

E2.1.10. Insurance Carrier. An insurance company issuing insurance through an association reinsuring or coinsuring such insurance.

E2.1.11. Insurance Product. A policy, annuity, or certificate of insurance issued by an insurer or evidence of insurance coverage issued by a self-insured association, including those with savings and investment features.

E2.1.12. Insurer. An entity licensed by the appropriate department to engage in the business of insurance.

E2.1.13. Military Services. See Joint Publication 1-02, "DoD Dictionary of Military and Associated Terms (Reference (e)).

E2.1.14. Normal Home Enterprises. Sales or services that are customarily conducted in a domestic setting and do not compete with an installation's officially sanctioned commerce.

E2.1.15. Personal Commercial Solicitation. Personal contact, to include meetings, meals, or telecommunications contact, for the purpose of seeking private business or trade.

E2.1.16. Securities. Mutual funds, stocks, bonds, or any product registered with the Securities and Exchange Commission except for any insurance or annuity product issued by a corporation subject to supervision by State insurance authorities.

E2.1.17. Suspension. Temporary termination of privileges pending completion of a commander's inquiry or investigation.

E2.1.18. Withdrawal. Termination of privileges for a set period of time following completion of a commander's inquiry or investigation.

### E3. ENCLOSURE 3

#### LIFE INSURANCE PRODUCTS AND SECURITIES

##### E3.1. LIFE INSURANCE PRODUCT CONTENT PREREQUISITES

Companies must provide DoD personnel a written description for each product or service they intend to market to DoD personnel on DoD installations. These descriptions must be written in a manner that DoD personnel can easily understand, and fully disclose the fundamental nature of the policy. Companies must be able to demonstrate that each form to be used has been filed with and approved, where applicable, by the insurance department of the State where the installation is located. Insurance products marketed to DoD personnel on overseas installations must conform to the standards prescribed by the laws of the state where the company is incorporated.

E3.1.1. Insurance products, other than certificates or other evidence of insurance issued by a self-insured association, offered and sold worldwide to personnel on DoD installations, must:

E3.1.1.1. Comply with the insurance laws of the State or country in which the installation is located and the requirements of this Instruction.

E3.1.1.2. Contain no restrictions by reason of Military Service or military occupational specialty of the insured, unless such restrictions are clearly indicated on the face of the contract.

E3.1.1.3. Plainly indicate any extra premium charges imposed by reason of Military Service or military occupational specialty.

E3.1.1.4. Contain no variation in the amount of death benefit or premium based upon the length of time the contract has been in force, unless all such variations are clearly described in the contract.

E3.1.1.5. In plain and readily understandable language, and in type font at least as large as the font used for the majority of the policy, inform Service members of:

E3.1.1.5.1. The availability and cost of government subsidized Servicemen's Group Life Insurance.

E3.1.1.5.2. The address and phone number where consumer complaints are received by the State insurance commissioner for the State in which the insurance product is being sold.

E3.1.1.5.3. That the U.S. Government has in no way sanctioned, recommended, or encouraged the sale of the product being offered. With respect to the sale or solicitation of insurance on Federal land or facilities located outside the United States, insurance products must contain the address and phone number where consumer complaints are received by the State insurance commissioner for the State which has issued the agent a resident license or the company is domiciled, as applicable.

E3.1.2. To comply with subparagraphs E3.1.1.2., E3.1.1.3. and E3.1.1.4., an appropriate reference stamped on the first page of the contract shall draw the attention of the policyholder to any restrictions by reason of Military Service or military occupational specialty. The reference shall describe any extra premium charges and any variations in the amount of death benefit or premium based upon the length of time the contract has been in force.

E3.1.3. Variable life insurance products may be offered provided they meet the criteria of the appropriate insurance regulatory agency and the Securities and Exchange Commission.

E3.1.4. Insurance products shall not be marketed or sold disguised as investments. If there is a savings component to an insurance product, the agent shall provide the customer written documentation, which clearly explains how much of the premium goes to the savings component per year broken down over the life of the policy. This document must also show the total amount per year allocated to insurance premiums. The customer must be provided a copy of this document that is signed by the insurance agent.

## E3.2. SALE OF SECURITIES

E3.2.1. All securities must be registered with the Securities and Exchange Commission.

E3.2.2. All sales of securities must comply with the appropriate Securities and Exchange Commission regulations.

E3.2.3. All securities representatives must apply to the commander of the installation on which they desire to solicit the sale of securities for permission to solicit.

E3.2.4. Where the accredited insurer's policy permits, an overseas accredited life insurance agent—if duly qualified to engage in security activities either as a registered representative of the National Association of Securities Dealers or as an associate of a broker or dealer registered with the Securities and Exchange Commission—may offer life insurance and securities for sale simultaneously. In cases of commingled sales, the allotment of pay for the purchase of securities cannot be made to the insurer.

## E3.3. USE OF THE ALLOTMENT OF PAY SYSTEM

E3.3.1. Allotments of military pay for life insurance products shall be made in accordance with Reference (o).

E3.3.2. For personnel in pay grades E-4 and below, in order to obtain financial counseling, at least seven calendar days shall elapse between the signing of a life insurance application and the certification of a military pay allotment for any supplemental commercial life insurance. Installation Finance Officers are responsible for ensuring this seven-day cooling-off period is monitored and enforced. The purchaser's commanding officer may grant a waiver of the seven-day cooling-off period requirement for good cause, such as the purchaser's imminent deployment or permanent change of station.

E3.4. ASSOCIATIONS – GENERAL

The recent growth and general acceptability of quasi-military associations offering various insurance plans to military personnel are acknowledged. Some associations are not organized within the supervision of insurance laws of either a State or the Federal Government. While some are organized for profit, others function as nonprofit associations under Internal Revenue Service regulations. Regardless of the manner in which insurance is offered to members, the management of the association is responsible for complying fully with the policies contained in this Instruction.



## E4. ENCLOSURE 4

### THE OVERSEAS LIFE INSURANCE REGISTRATION PROGRAM

#### E4.1. REGISTRATION CRITERIA

##### E4.1.1. Initial Registration

E4.1.1.1. Insurers must demonstrate continuous successful operation in the life insurance business for a period of not less than 5 years on December 31 of the year preceding the date of filing the application.

E4.1.1.2. Insurers must be listed in Best's Life-Health Insurance Reports and be assigned a rating of B+ (Very Good) or better for the business year preceding the Government's fiscal year for which registration is sought.

##### E4.1.2. Re-registration

E4.1.2.1. Insurers must demonstrate continuous successful operation in the life insurance business, as described in paragraph E4.1.1.1.

E4.1.2.2. Insurers must retain a Best's rating of B+ or better, as described in subparagraph E4.1.1.2.

E4.1.2.3. Insurers must demonstrate a record of compliance with the policies found in this Instruction. .

E4.1.3. Waiver Provisions. Waivers of the initial registration or re-registration provisions shall be considered for those insurers demonstrating substantial compliance with the aforementioned criteria.

#### E4.2. APPLICATION INSTRUCTIONS

E4.2.1. Applications Filed Annually. Insurers must apply by June 30 of each year for solicitation privileges on overseas U.S. military installations for the next fiscal year beginning October 1. Applications e-mailed, faxed, or postmarked after June 30 shall not be considered.

E4.2.2. Application Prerequisites. A letter of application, signed by the President, Vice President, or designated official of the insurance company shall be forwarded to the Principal Deputy Under Secretary of Defense (Personnel and Readiness), Attention: Morale, Welfare and Recreation (MWR) Policy Directorate, 4000 Defense, Pentagon, Washington, DC 20301-4000. The registration criteria in paragraph E4.1.1. or E4.1.2., above, must be met to satisfy application prerequisites. The letter shall contain the information set forth below, submitted in the order listed. Where criteria are not applicable, the letter shall so state.

E4.2.2.1. The overseas Combatant Commands (e.g., U.S. European Command, U.S. Pacific Command, U.S. Central Command, and U.S. Southern Command) where the company presently solicits, or plans to solicit, on U.S. military installations.

E4.2.2.2. A statement that the company has complied with, or shall comply with, the applicable laws of the country or countries wherein it proposes to solicit. "Laws of the country" means all national, provincial, city, or county laws or ordinances of any country, as applicable.

E4.2.2.3. A statement that the products to be offered for sale conform to the standards prescribed in Enclosure 3 and contain only the standard provisions such as those prescribed by the laws of the State where the company's headquarters are located.

E4.2.2.4. A statement that the company shall assume full responsibility for the acts of its agents with respect to solicitation. If warranted, the number of agents may be limited by the overseas command concerned.

E4.2.2.5. A statement that the company shall only use agents who have been licensed by the appropriate State and registered by the overseas command concerned to sell to DoD personnel on DoD installations.

E4.2.2.6. Any explanatory or supplemental comments that shall assist in evaluating the application.

E4.2.2.7. If the Department of Defense requires facts or statistics beyond those normally involved in registration, the company shall make separate arrangements to provide them.

E4.2.2.8. A statement that the company's general agent and other registered agents are appointed in accordance with the prerequisites established in section E4.3.

E4.2.3. If a company is a life insurance company subsidiary, it must be registered separately on its own merits.

#### E4.3. AGENT REQUIREMENTS

The overseas Combatant Commanders shall apply the following principles in registering agents:

E4.3.1. An agent must possess a current State license. This requirement may be waived for a registered agent continuously residing and successfully selling life insurance in foreign areas, who, through no fault of his or her own, due to State law (or regulation) governing domicile requirements, or requiring that the agent's company be licensed to do business in that State, forfeits eligibility for a State license. The request for a waiver shall contain the name of the State or jurisdiction that would not renew the agent's license.

E4.3.2. General agents and agents may represent only one registered commercial insurance company. This principle may be waived by the overseas Combatant Commander if multiple representations are in the best interest of DoD personnel.

E4.3.3. An agent must have at least 1 year of successful life insurance underwriting experience in the United States or its territories, generally within the 5 years preceding the date of application, in order to be approved for overseas solicitation.

E4.3.4. The overseas Combatant Commanders may exercise further agent control procedures as necessary.

E4.3.5. An agent, once registered in an overseas area, may not change affiliation from the staff of one general agent to another and retain registration, unless the previous employer certifies in writing that the release is without justifiable prejudice. Overseas Combatant Commanders will have final authority to determine justifiable prejudice. Indebtedness of an agent to a previous employer is an example of justifiable prejudice.

#### E4.4. ANNOUNCEMENT OF REGISTRATION

E4.4.1. Registration by the Department of Defense upon annual applications of insurers shall be announced as soon as practicable by notice to each applicant and by a list released annually in September to the appropriate overseas Combatant Commanders. Approval does not constitute DoD endorsement of the insurer or its products. Any advertising by insurers or verbal representation by its agents, which suggests such endorsement, is prohibited.

E4.4.2. In the event registration is denied, specific reasons for the denial shall be provided to the applicant.

E4.4.2.1. The insurer shall have 30 days from the receipt of notification of denial of registration (sent certified mail, return receipt requested) in which to request reconsideration of the original decision. This request must be in writing and accompanied by substantiating data or information in rebuttal of the specific reasons upon which the denial was based.

E4.4.2.2. Action by the Office of the PDUSD(P&R) on a request for reconsideration is final.

E4.4.2.3. An applicant that is presently registered as an insurer shall have 90 calendar days from final action denying registration in which to close operations.

E4.4.3. Upon receiving an annual letter approving registration, each company shall send to the applicable overseas Combatant Commander a verified list of agents currently registered for overseas solicitation. Where applicable, the company shall also include the names and prior military affiliation of new agents for whom original registration and permission to solicit on base is requested. Insurers initially registered shall be furnished instructions by the Department of Defense for agent registration procedures in overseas areas.

E4.4.4. Material changes affecting the corporate status and financial condition of the company that occur during the fiscal year of registration must be reported to the MWR Policy Directorate at the address in paragraph E4.2.2 as they occur.

E4.4.4.1. The Office of the PDUSD(P&R) reserves the right to terminate registration if such material changes appear to substantially affect the financial and operational standards described in section E4.1. on which registration was based.

E4.4.4.2. Failure to report such material changes may result in termination of registration regardless of how it affects the standards.

E4.4.5. If an analysis of information furnished by the company indicates that unfavorable trends are developing that could adversely affect its future operations, the Office of the PDUSD(P&R) may, at its option, bring such matters to the attention of the company and request a statement as to what action, if any, is considered to deal with such unfavorable trends.

E5. ENCLOSURE 5PERSONAL COMMERCIAL SOLICITATION EVALUATION

PERSONAL COMMERCIAL SOLICITATION EVALUATION			
<b>PRIVACY ACT STATEMENT</b>			
AUTHORITY: Section 301 of Title 5 U.S.C.			
<p><b>PRINCIPAL PURPOSE(S):</b> Information on this form will be used to document the experience with the sales representative who provides the Service member with this evaluation. This information will be maintained at the installation level. It may be forwarded to officials within the Department of Defense responsible for oversight of personal commercial solicitation practices if further action is required. These officials may need to make contact concerning the solicitation described in questions 2, 3, and 4. Service member response will help ensure sales representatives conduct themselves fairly and in accordance with DoD Instruction 1344.7. This information will be maintained as part of a case file in the event proceedings are considered necessary to deny or withdraw permission for the sales representative and/or the company to solicit on one or more installations.</p>			
ROUTINE USE(S): None.			
DISCLOSURE: Voluntary. There is no consequence to the Service member for not completing this evaluation.			
<p>Please take a moment to respond to the following questions concerning your experience with the sales representative who provided you this evaluation. Your response will help ensure sales representatives conduct themselves fairly and according to the policies outlined in DoD Instruction 1344.7.</p> <p><b>When you have completed this evaluation, please send it to the Installation Commander or his/her designated representative. Please do not give the completed evaluation back to the sales representative to mail for you.</b></p>			
<b>1. SALES REPRESENTATIVE WHO CONTACTED YOU AND HIS OR HER COMPANY</b>			
a. NAME OF SALES REPRESENTATIVE		b. COMPANY NAME	
Harry Cotter		All American Life Insurance Company	
<b>2. MAKING THE APPOINTMENT</b> (Mark (X) "Yes" if any of the following are true)			
a. The sales representative failed to make an appointment in advance to see me.			YES NO
			X
b. The initial contact to schedule an appointment occurred while I was on duty (during normal duty hours).			X
c. My initial contact with the sales representative was in response to a notice in an official installation bulletin, marquee, announcement or newsletter that said he or she would be on the installation during a specific time or at a specific place.			X
d. A superior in my chain of command advised or required me to meet with the sales representative.			X
e. The sales representative made initial contact with me via a government phone, fax, or computer.			X
<b>3. TIME AND PLACE OF THE APPOINTMENT</b> (Mark (X) "Yes" if any of the following are true)			YES NO
a. The sales presentation took place on the installation while I was on duty (during normal duty hours).			X
b. The sales presentation took place during a mandatory group meeting with other DoD personnel or as part of a military service sponsored financial education program.			X
c. The sales presentation took place in an unauthorized or restricted area.			X
d. The sales representative used an on-base facility as a showroom to display his or her product or services. (This does not include displays conducted by military family members in their on-base residence.)			X
<b>4. CONDUCT DURING THE APPOINTMENT</b> (Mark (X) "Yes" if any of the following are true)			YES NO
a. I was unduly pressured to buy the product or service.			X
b. I was not given the adequate facts, or was induced to purchase based on factors other than the merits of the product or service.			X
c. I was offered an incentive to meet with the sales representative, purchase the product or service, or drop a competing offer.			X
d. The sales representative is a DoD employee of senior rank.			X
e. The sales representative implied that he or she is sponsored or endorsed by the military, the installation or my unit. (For example, the representative used an official or unofficial title such as "unit advisor" or "installation consultant.")			X
f. The sales representative had a military pay allotment or direct deposit form in his/her possession, or requested "MyPay" account access or PIN number.			X
<b>5. YOUR CONTACT INFORMATION</b>			
a. NAME (Last, First, Middle Initial)		b. HOME TELEPHONE NUMBER (Include area code)	c. WORK TELEPHONE NUMBER (Include area code)
Hargrove, Harold H.		(901) 336-1001	(901) 436-8988
d. E-MAIL ADDRESS		e. UNIT ADDRESS	
hhh@coastal.com		329 Inf Bn (ABN), Fort Bragg, NC 28307	

DD FORM 2885, APR 2006

FormFlow/Adobe Professional 6.0



Department of Defense

# DIRECTIVE

NUMBER 6400.1

August 23, 2004

---

---

PDUSD(P&R)

SUBJECT: Family Advocacy Program (FAP)

References: (a) DoD Directive 6400.1, subject as above, June 23, 1992 (hereby canceled)  
(b) DoD 5025.1-M, "DoD Directives System Procedures," March 5, 2003  
(c) DoD Instruction 6400.2, "Child and Spouse Abuse Report,"  
July 10, 1987 (hereby canceled)  
(d) DoD Directive 1030.1, "Victim and Witness Assistance," April 13, 2004  
(e) DoD Directive 6025.13, "Medical Quality Assurance (MQA) in the  
Military Health System (MHS)," May 4, 2004  
(f) Section 1787 of title 10, United States Code

## 1. REISSUANCE AND PURPOSE

1.1. This Directive administratively reissues reference (a) to update:

1.1.1. DoD policy on child abuse and neglect (hereafter referred to as "child abuse" and spouse abuse).

1.1.2. The DoD Family Advocacy Program (FAP).

1.1.3. Responsibilities for the establishment, operation, and use of programs designed to address child and spouse abuse.

1.2. This Directive authorizes DoD publications on the FAP consistent with reference (b).

1.3. Cancels reference (c).

1.4. Provides internal DoD guidance to protect and assist actual or alleged victims of child and spouse abuse. It is not intended to and does not create any rights, substantive or procedural, enforceable at law by any victim, witness, suspect, accused, or other person in any matter, civil or criminal. No limitations are placed on the lawful

prerogatives of the Department of Defense or its officials. DoD policy governing the protection of victims and witnesses is prescribed in DoD Directive 1030.1 (reference (d)).

## 2. APPLICABILITY AND SCOPE

This Directive:

2.1. Applies to the Office of the Secretary of Defense and the Military Departments, the Chairman of the Joint Chiefs of Staff, the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the "DoD Components"). The term "Military Services," as used herein, refers to the Army, the Navy, the Air Force, and the Marine Corps.

2.2. Encompasses all persons eligible to receive treatment in military medical treatment facilities.

## 3. DEFINITIONS

Terms used in this Directive are defined in enclosure 1.

## 4. POLICY

It is DoD policy to:

4.1. Prevent child abuse and domestic abuse involving persons identified in section 2., above, through public awareness, education, and family support programs provided by the FAP, and through standardized FAP programs and activities for military families who have been identified as at-risk of committing child abuse or domestic abuse.

4.2. Promote early identification and coordinated, comprehensive intervention, assessment, and support to persons identified in section 2., above, who are victims of suspected child abuse or domestic abuse, as defined by this Directive.

4.3. Provide appropriate resource and referral information to persons not identified in section 2., above, who are victims of alleged child abuse or domestic abuse.

4.4. Provide assessment, rehabilitation, and treatment, including comprehensive abuser intervention, that supplement appropriate administrative or disciplinary action, to persons identified in section 2., above, who are alleged to have committed child abuse and domestic abuse.

4.5. Cooperate with responsible civilian authorities and organizations in efforts to address the problems to which this Directive applies.

4.6. Cooperate with responsible civilian authorities in efforts to address the problems to which this Directive applies.

## 5. RESPONSIBILITIES

5.1. The Principal Deputy Under Secretary of Defense for Personnel and Readiness (PDUSD(P&R)), under the Under Secretary of Defense for Personnel and Readiness shall:

5.1.1. Develop a coordinated approach to family advocacy issues consistent with this Directive, recognizing that programs shall be designed to meet local needs.

5.1.2. Develop criteria for determining the minimum number of appropriately trained professionals, counselors, and support staff, and the range of services required to ensure program effectiveness.

5.1.3. Coordinate the management of this program with similar medical and social programs serving military families.

5.1.4. Program, budget, and allocate funds and other resources for the FAP.

5.1.5. Collect and analyze FAP data.

5.1.6. Serve on Federal committees and advisory groups that encompass issues included in the FAP.

5.1.7. Assist the Military Services in their efforts to establish, develop, and maintain comprehensive FAPs.

5.1.8. Collaborate with the DoD Components to establish FAP standards.

5.1.9. Monitor and evaluate existing FAPs at the headquarters level.

5.1.10. Provide guidance and technical assistance.

5.1.11. Collaborate with Federal and State agencies that address family advocacy issues.

5.1.12. Facilitate the identification and resolution of joint-Service issues and concerns.



5.1.13. Monitor compliance with this Directive.

5.2. The Secretaries of the Military Departments shall:

5.2.1. Establish broad policies on the development of FAPs. Those policies shall include, but not be limited to, the prohibition of child and spouse abuse by persons identified in section 2., above.

5.2.2. Identify the fiscal and personnel resources necessary to implement the FAP, and report these resource totals to the Office of the PDUSD(P&R).

5.2.3. Designate a FAP manager.

5.2.4. Coordinate efforts and resources among all activities serving families to promote the optimal delivery of services.

5.2.5. Provide program and obligation data, as required, to the Office of the PDUSD(P&R).

5.2.6. Establish standardized criteria, in accordance with DoD Directive 6025.13 (reference (e)), for the selection and certification of healthcare and social service personnel who counsel individuals and families as part of the FAP.

5.2.7. Provide education and training to key personnel on this policy and effective measures to alleviate problems associated with child and spouse abuse.

5.2.8. Encourage local commands to develop memoranda of understanding providing for cooperation and reciprocal reporting of information with the appropriate civilian officials, in accordance with Section 1787 of title 10, United States Code (reference (f)).

5.2.9. Ensure eligible military families living in the civilian community and on military installations are included in the FAP.

5.2.10. Ensure that installation commanders appoint FAP officers to implement local FAPs, in accordance with enclosure 2 of this Directive.

5.2.11. Ensure that installation commanders establish family advocacy case review committees, in accordance with enclosure 2, and provide appropriate training to the members.

5.2.12. Ensure the development of additional guidelines for assembling complete case information under enclosure 2 of this Directive.

5.2.13. Develop specific criteria for retaining members in military service who have been involved in an incident of substantiated abuse.


5.2.14. Develop guidelines for case management and monitoring of the FAP.

6. INFORMATION REQUIREMENTS

The "DoD Child Maltreatment and Domestic Abuse Incident Report," is assigned Report Control Symbol DD-FM&P(SA)2052. The Secretaries of the Military Departments shall submit this data to the Defense Manpower Data Center no later than 20 days after the end of each calendar year quarter.

7. EFFECTIVE DATE

This Directive is effective immediately.



Paul Wolfowitz  
Deputy Secretary of Defense

Enclosures - 2

E1. Definitions

E2. Guidance for the FAP

## E1. ENCLOSURE 1

### DEFINITIONS

E1.1.1. Case Review Committee (CRC). A multidisciplinary team of designated individuals working at the installation level, tasked with the evaluation and determination of abuse and/or neglect cases and the development and coordination of treatment and disposition recommendations.

E1.1.2. Case Status. The status of the case at the time of the report. Includes "substantiated," "suspected," or "unsubstantiated," as follows:

E1.1.2.1. Substantiated. A case that has been investigated and the preponderance of available information indicates that abuse has occurred. The information that supports the occurrence of abuse is of greater weight or more convincing than the information indicating that abuse did not occur.

E1.1.2.2. Suspected. A case determination is pending further investigation. Duration for a case to be "suspected" and under investigation should not exceed 12 weeks.

E1.1.2.3. Unsubstantiated. An alleged case that has been investigated and the available information is insufficient to support the claim that child abuse and/or neglect or spouse abuse did occur. The family needs no family advocacy services.

E1.1.3. Child Abuse and/or Neglect. Includes physical injury, sexual maltreatment, emotional maltreatment, deprivation of necessities, or combinations for a child by an individual responsible for the child's welfare under circumstances indicating that the child's welfare is harmed or threatened. The term encompasses both acts and omissions on the part of a responsible person. A "child" is a person under 18 years of age for whom a parent, guardian, foster parent, caretaker, employee of a residential facility, or any staff person providing out-of-home care is legally responsible. The term "child" means a natural child, adopted child, stepchild, foster child, or ward. The term also includes an individual of any age who is incapable for self-support because of a mental or physical incapacity and for whom treatment in a medical treatment facility (MTF) is authorized.

E1.1.4. Family Advocacy Program (FAP). A program designed to address prevention, identification, evaluation, treatment, rehabilitation, follow-up, and reporting of family violence. FAPs consist of coordinated efforts designed to prevent and intervene in cases of family distress, and to promote healthy family life.

E1.1.5. FAP Manager. An individual designated by the Secretary of the Military Department to manage, monitor, and coordinate the FAP at the headquarters level.

E1.1.6. FAP Officer. A designated officer who manages, monitors, and provides staff supervision of the FAP at the local level.

E1.1.7. Spouse Abuse. Includes assault, battery, threat to injure or kill, other act of force or violence, or emotional maltreatment inflicted on a partner in a lawful marriage when one of the partners is a military member or is employed by the Department of Defense and is eligible for treatment in an MTF. A spouse under 18 years of age shall be treated in this category.

**E2. ENCLOSURE 2**

**GUIDANCE ON THE FAP**

E2.1.1. When assisting victims of child and spouse abuse and witnesses to such acts, attention shall be given to the applicable provisions of reference (d). Local response to cases of suspected child or spouse abuse shall be coordinated among appropriate military and civilian agencies to ensure that any further trauma to the victim(s) is minimized. When an act of abuse allegedly has occurred, the local FAP office shall be notified immediately and shall, in turn, ensure implementation of the following procedures:

E2.1.1.1. Medical assessment and treatment for all family members by appropriately trained personnel.

E2.1.1.2. Notification of the Service member's commanding officer, military law enforcement, and investigative agencies.

E2.1.1.3. Notification of the local public child protective agency (in alleged child abuse cases only) in the United States and, where covered by agreement, overseas.

E2.1.1.4. Observance of the applicable rights of alleged offenders.

E2.1.2. The CRC that accesses reports of alleged child and spouse abuse shall review all the available case material and shall make a status determination of "substantiated," "suspected," or "unsubstantiated" for each case. The CRC shall make recommendations to the Service member's commanding officer on inclusion in a treatment program. The CRC shall monitor and advise the commander of progress in treatment.

E2.1.3. Guidelines shall be developed locally to ensure that commanders have timely access to complete case information when considering appropriate disposition of allegations. Factors that shall be considered in determining dispositions to include the following:

E2.1.3.1. Military performance and potential for further useful service.

E2.1.3.2. Prognosis for treatment, as determined by a clinician with expertise in the diagnosis and management of the abuse at issue (child abuse, child neglect, child sexual abuse, and/or spouse abuse).

E2.1.3.3. Extent to which the alleged offender accepts responsibility for his or her behavior and expresses a genuine desire for treatment.

E2.1.3.5. All alleged offenders and their families shall have access to appropriate case management and treatment services.



# Department of Defense

## DIRECTIVE

NUMBER 8500.01E

October 24, 2002

Certified Current as of April 23, 2007

---

---

ASD(NII)/DoD CIO

SUBJECT: Information Assurance (IA)

- References: (a) Section 2224 of title 10, United States Code, "Defense Information Assurance Program"
- (b) DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988 (hereby canceled)
  - (c) DoD 5200.28-M, "ADP Security Manual," January 1973 (hereby canceled)
  - (d) DoD 5200.28-STD, "DoD Trusted Computer Security Evaluation Criteria," December 1985 (hereby canceled)
  - (e) through (ah), see enclosure 1

### 1. PURPOSE

This Directive:

1.1. Establishes policy and assigns responsibilities under reference (a) to achieve Department of Defense (DoD) information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare.

1.2. Supersedes DoD Directive 5200.28, DoD 5200.28-M, DoD 5200.28-STD, and DoD Chief Information Officer (CIO) Memorandum 6-8510 (references (b), (c), (d), and (e)).

1.3. Designates the Secretary of the Army as the Executive Agent for the integration of common biometric technologies throughout the Department of Defense.

1.4. Authorizes the publication of DoD 8500.1-M consistent with DoD 5025.1-M (reference (f)).

## 2. APPLICABILITY AND SCOPE

### 2.1. This Directive applies to:

2.1.1. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as "the DoD Components").

2.1.2. All DoD-owned or -controlled information systems that receive, process, store, display or transmit DoD information, regardless of mission assurance category, classification or sensitivity, including but not limited to:

2.1.2.1. DoD information systems that support special environments, e.g., Special Access Programs (SAP) and Special Access Requirements (SAR), as supplemented by the special needs of the program.

2.1.2.2. Platform IT interconnections, e.g., weapons systems, sensors, medical technologies or utility distribution systems, to external networks.

2.1.2.3. Information systems under contract to the Department of Defense.

2.1.2.4. Outsourced information-based processes such as those supporting e-Business or e-Commerce processes.

2.1.2.5. Information systems of Nonappropriated Fund Instrumentalities.

2.1.2.6. Stand-alone information systems.

2.1.2.7. Mobile computing devices such as laptops, handhelds, and personal digital assistants operating in either wired or wireless mode, and other information technologies as may be developed.

2.2. Nothing in this policy shall alter or supercede the existing authorities and policies of the Director of Central Intelligence (DCI) regarding the protection of Sensitive Compartmented Information (SCI) and special access programs for intelligence as directed by Executive Order 12333 (reference (g)) and other laws and regulations.

2.3. This policy does not apply to weapons systems as defined by DoD Directive 5144.1 (reference (h)) or other IT components, both hardware and software, that are physically part of, dedicated to, or essential in real time to a platform's mission performance where there is no platform IT interconnection.



### 3. DEFINITIONS

Terms used in this Directive are defined in National Security Telecommunications and Information Systems Security Instruction Number 4009 (reference (i)) or enclosure 2.

### 4. POLICY

It is DoD policy that:

4.1. Information assurance requirements shall be identified and included in the design, acquisition, installation, operation, upgrade, or replacement of all DoD information systems in accordance with 10 U.S.C. Section 2224, Office of Management and Budget Circular A-130, Appendix III, DoD Directive 5000.1 (references (a), (j), and (k)), this Directive, and other IA-related DoD guidance, as issued.

4.2. All DoD information systems shall maintain an appropriate level of confidentiality, integrity, authentication, non-repudiation, and availability that reflect a balance among the importance and sensitivity of the information and information assets; documented threats and vulnerabilities; the trustworthiness of users and interconnecting systems; the impact of impairment or destruction to the DoD information system; and cost effectiveness. For IA purposes all DoD information systems shall be organized and managed in the four categories defined in enclosure 2: automated information system (AIS) applications, enclaves (which include networks), outsourced IT-based processes, and platform IT interconnections.

4.3. Information assurance shall be a visible element of all investment portfolios incorporating DoD-owned or -controlled information systems, to include outsourced business processes supported by private sector information systems and outsourced information technologies; and shall be reviewed and managed relative to contributions to mission outcomes and strategic goals and objectives, in accordance with 40 U.S.C. Sections 1423 and 1451 (reference (l)). Data shall be collected to support reporting and IA management activities across the investment life cycle.

4.4. Interoperability and integration of IA solutions within or supporting the Department of Defense shall be achieved through adherence to an architecture that will enable the evolution to network centric warfare by remaining consistent with the Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance Architecture Framework, and a defense-in-depth approach. This combination produces layers of technical and non-technical solutions that: provide appropriate levels of confidentiality, integrity, authentication, non-repudiation, and availability; defend the perimeters of enclaves; provide appropriate degrees of protection to all enclaves and computing environments; and make appropriate use of supporting IA infrastructures, to include robust key management and incident detection and response.

4.5. The Department of Defense shall organize, plan, assess, train for, and conduct the defense of DoD computer networks as integrated computer network defense (CND) operations that are coordinated across multiple disciplines in accordance with DoD Directive O-8530.1 (reference (m)).

4.6. Information assurance readiness shall be monitored, reported, and evaluated as a distinguishable element of mission readiness throughout all the DoD Components, and validated by the DoD CIO.

4.7. All DoD information systems shall be assigned a mission assurance category that is directly associated with the importance of the information they contain relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. Requirements for availability and integrity are associated with the mission assurance category, while requirements for confidentiality are associated with the information classification or sensitivity and need-to-know. Both sets of requirements are primarily expressed in the form of IA controls and shall be satisfied by employing the tenets of defense-in-depth for layering IA solutions within a given IT asset and among assets; and ensuring appropriate robustness of the solution, as determined by the relative strength of the mechanism and the confidence that it is implemented and will perform as intended. The IA solutions that provide availability, integrity, and confidentiality also provide authentication and non-repudiation.

4.8. Access to all DoD information systems shall be based on a demonstrated need-to-know, and granted in accordance with applicable laws and DoD 5200.2-R (reference (n)) for background investigations, special access and IT position designations and requirements. An appropriate security clearance and non-disclosure agreement are also required for access to classified information in accordance with DoD 5200.1-R (reference (o)). Further:

4.8.1. The minimum requirement for DoD information system access shall be a properly administered and protected individual identifier and password.

4.8.2. The use of Public Key Infrastructure (PKI) certificates and biometrics for positive authentication shall be in accordance with published DoD policy and procedures. These technologies shall be incorporated in all new acquisitions and upgrades whenever possible. Where interoperable PKI is required for the exchange of unclassified information with vendors and contractors, the Department of Defense shall only accept PKI certificates obtained from a DoD-approved external certificate authority or other mechanisms approved in accordance with DoD policy.

4.9. In addition to the requirements in paragraph 4.8., foreign exchange personnel and representatives of foreign nations, coalitions or international organizations may be authorized access to DoD information systems containing classified or sensitive information only if all of the following conditions are met:

4.9.1. Access is authorized only by the DoD Component Head in accordance with the Department of Defense, the Department of State (DoS), and DCI disclosure and interconnection policies, as applicable.

4.9.2. Mechanisms are in place to strictly limit access to information that has been cleared for release to the represented foreign nation, coalition or international organization, (e.g., North Atlantic Treaty Organization) in accordance with DoD Directive 5230.11 (reference (p)), for classified information, and other policy guidance for unclassified information such as reference (o), DoD Directive 5230.20E (reference (q)), and DoD Instruction 5230.27 (reference (r)).

4.10. Authorized users who are contractors, DoD direct or indirect hire foreign national employees, or foreign representatives as described in paragraph 4.9., above, shall always have their affiliation displayed as part of their e-mail addresses.

4.11. Access to DoD-owned, -operated or -outsourced web sites shall be strictly controlled by the web site owner using technical, operational, and procedural measures appropriate to the web site audience and information classification or sensitivity.

4.11.1. Access to DoD-owned, -operated or -controlled web sites containing official information shall be granted according to reference (o) and need-to-know rules established by the information owner.

4.11.2. Access to DoD-owned, -operated or -controlled web sites containing public information is not restricted; however, the information accessible through the web sites shall be limited to unclassified information that has been reviewed and approved for release in accordance with DoD Directive 5230.9 and DoD Instruction 5230.29 (references (s) and (t)).

4.12. DoD information systems shall regulate remote access and access to the Internet by employing positive technical controls such as proxy services and screened subnets, also called demilitarized zones (DMZ), or through systems that are isolated from all other DoD information systems through physical means. This includes remote access for telework.

4.13. All DoD information systems shall be certified and accredited in accordance with DoD Instruction 5200.40 (reference (u)).

4.14. All interconnections of DoD information systems shall be managed to continuously minimize community risk by ensuring that the assurance of one system is not undermined by vulnerabilities of interconnected systems.

4.14.1. Interconnections of Intelligence Community (IC) systems and DoD information systems shall be accomplished using a process jointly established by the DoD CIO and the IC CIO.

4.14.2. Connection to the Defense Information System Network (DISN) shall comply with connection approval procedures and processes, as established.

4.14.3. Interconnections among DoD information systems of different security domains or with other U.S. Government systems of different security domains shall be employed only to meet compelling operational requirements, not operational convenience. Secure configurations of approved IA and IA-enabled IT products, uniform risk criteria, trained systems security personnel, and strict configuration control shall be employed. The community risk shall be assessed and measures taken to mitigate that risk in accordance with procedures established by the DISN Designated Approving Authorities (DAAs) prior to interconnecting the systems.

4.14.4. The interconnection of DoD information systems with those of U.S. allies, foreign nations, coalition partners, or international organizations shall comply with applicable international agreements and, whenever possible, DoD IA policies. Variations shall be approved by the responsible Combatant Commander and the DISN DAAs, and incorporated in the system security documentation. Information provided through these interconnections must be released in accordance with reference (o) or reference (p).

4.15. All DoD information systems shall comply with DoD ports and protocols guidance and management processes, as established.

4.16. The conduct of all DoD communications security activities, including the acquisition of COMSEC products, shall be in accordance with DoD Directive C-5200.5 (reference (v)).

4.17. All IA or IA-enabled IT hardware, firmware, and software components or products incorporated into DoD information systems must comply with the evaluation and validation requirements of National Security Telecommunications and Information Systems Security Policy Number 11 (reference (w)). Such products must be satisfactorily evaluated and validated either prior to purchase or as a condition of purchase; i.e., vendors will warrant, in their responses to a solicitation and as a condition of the contract, that the vendor's products will be satisfactorily validated within a period of time specified in the solicitation and the contract. Purchase contracts shall specify that product validation will be maintained for updated versions or modifications by subsequent evaluation or through participation in the National IA Partnership (NIAP) Assurance Maintenance Program.

4.18. All IA and IA-enabled IT products incorporated into DoD information systems shall be configured in accordance with DoD-approved security configuration guidelines.<sup>1</sup>

4.19. Public domain software products, and other software products with limited or no warranty, such as those commonly known as freeware or shareware, shall only be used in DoD information systems to meet compelling operational requirements. Such products shall be thoroughly assessed for risk and accepted for use by the responsible DAA.

---

<sup>1</sup> Guidelines are available at <http://iase.disa.mil/> and <http://www.nsa.gov/>

4.20. DoD information systems shall be monitored based on the assigned mission assurance category and assessed risk in order to detect, isolate, and react to intrusions, disruption of services, or other incidents that threaten the IA of DoD operations or IT resources, including internal misuse. DoD information systems also shall be subject to active penetrations and other forms of testing used to complement monitoring activities in accordance with DoD and Component policy and restrictions.

4.21. Identified DoD information system vulnerabilities shall be evaluated for DoD impact, and tracked and mitigated in accordance with DoD-directed solutions, e.g., Information Assurance Vulnerability Alerts.

4.22. All personnel authorized access to DoD information systems shall be adequately trained in accordance with DoD and Component policies and requirements and certified as required in order to perform the tasks associated with their IA responsibilities.

4.23. Individuals shall be notified of their privacy rights and security responsibilities in accordance with DoD Component General Counsel-approved processes when attempting access to DoD information systems.

4.24. Mobile code technologies shall be categorized and controlled to reduce their threat to DoD information systems in accordance with DoD and Component policy and guidance.

4.25. A DAA shall be appointed for each DoD information system operating within or on behalf of the Department of Defense, to include outsourced business processes supported by private sector information systems and outsourced information technologies. The DAA shall be a U.S. citizen, a DoD employee, and have a level of authority commensurate with accepting, in writing, the risk of operating DoD information systems under his or her purview.

4.26. All military voice radio systems, to include cellular and commercial services, shall be protected consistent with the classification or sensitivity of the information transmitted on the system.

## 5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for *Networks and Information Integration*, as the DoD Chief Information Officer, shall:

5.1.1. Monitor, evaluate and provide advice to the Secretary of Defense regarding all DoD IA activities.

5.1.2. Oversee appropriations earmarked for the DoD IA program and manage the supporting activities of the office of the Defense-wide Information Assurance Program (DIAP) Office in accordance with reference (a).

5.1.3. Develop and promulgate additional IA policy guidance consistent with this Directive to address such topics as ports and protocols management, vulnerability management, biometrics, security management, IA education and training, mobile code, and interconnection between security domains.

5.1.4. Ensure the integration of IA initiatives with critical infrastructure protection sector liaisons, as defined in DoD Directive 3020.40 (reference (x)).

5.1.5. Establish a formal coordination process with the IC CIO to ensure proper protection of IC information within the Department of Defense.

5.1.6. Establish metrics and annually validate the IA readiness of all DoD Components as an element of mission readiness.

5.1.7. Ensure that responsibilities for IA aspects of Major Defense Acquisition Program design are integrated into existing Under Secretary of Defense (Acquisition, Technology, and Logistics) (USD(AT&L)) and Service Acquisition Executive processes.

5.1.8. Require the Director, Defense Information Systems Agency (DISA) to:

5.1.8.1. Develop, implement and oversee a single IA approach for layered protection (defense-in-depth) of the DISN in coordination with the Chairman of the Joint Chiefs of Staff, Director, Defense Intelligence Agency (DIA) and Director, National Security Agency (NSA).

5.1.8.2. Establish and manage connection approval processes for the DISN.

5.1.8.3. Develop and provide IA training and awareness products.

5.1.8.4. Develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA.

5.1.8.5. Establish and implement:

5.1.8.5.1. A DoD ports and protocols management process.

5.1.8.5.2. Procedures for mitigation of risks associated with the use of mobile code in DoD information systems.

5.1.8.5.3. A web-based resource providing access to current DoD and Federal IA and IA-related policy and guidance, including recent and pending legislation.

5.1.9. Require the Director, Defense Intelligence Agency to:

5.1.9.1. Provide finished intelligence on IA, including threat assessments, to the DoD Components.

5.1.9.2. Develop, implement, and oversee an IA program for layered protection of the DoD non-cryptologic SCI systems including the DoD Intelligence Information System (DoDIIS) on the basis of defined DoD information systems and geographical or organizational boundaries.

5.1.9.3. Certify and accredit DoD non-cryptologic SCI and DoDIIS applications, enclaves, platform IT interconnections, and outsourced IT-based processes, and develop and provide an IA education, training, and awareness program for DoD non-cryptologic SCI systems and DoDIIS users and administrators.

5.1.9.4. Establish and manage a connection-approval process for the Joint Worldwide Intelligence Communications System.

5.1.10. Require the Director, Defense Security Service to monitor information system security practices and conduct regular inspections of DoD contractors processing classified information in accordance with DoD 5220.22-M (reference (y)).

5.2. The Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) shall:

5.2.1. Require the Director, Defense Research and Engineering (DDR&E) to:

5.2.1.1. Monitor and oversee, in coordination with the Defense-wide Information Assurance Program Office, all Defense-wide IA research and technology investments and activities to include protection mechanisms, detection and monitoring, response and recovery, and IA assessment tools and techniques.

5.2.1.2. Require the Director, Defense Advanced Research Projects Agency (DARPA) to coordinate all DoD IA research and technology initiatives under DARPA's purview with the Director, NSA.

5.2.2. Integrate policies established by this Directive and reference (w) into acquisition policy and guidance to include the Federal Acquisition Regulations System (reference (z)), and incorporate such policies into acquisitions under his or her purview.

5.2.3. Oversee IA assessments, in coordination with the Director, Operational Testing and Evaluation.



5.3. The Under Secretary of Defense for Personnel and Readiness shall, in coordination with the ASD(*NI*), develop and implement IA personnel management and skill tracking procedures and processes to ensure adequate personnel resources are available to meet critical DoD IA requirements.

5.4. The OSD Principal Staff Assistants shall:

5.4.1. Ensure end-to-end protection of information flows in their functional areas by guiding investments and other actions relating to IA.

5.4.2. Ensure that IA requirements for DoD information systems developed under their cognizance are fully coordinated at the DoD Component level and with the DIAP.

5.4.3. Appoint DAAs for Joint and Defense-wide information systems under their purview (e.g., the Defense Civilian Personnel Data System, Defense Message System, Defense Travel System, and the Joint Total Asset Visibility System).

5.4.4. Identify and include IA requirements in the design, acquisition, installation, operation, upgrade or replacement of all DoD information systems under their purview.

5.5. The Secretary of the Army shall serve as the Executive Agent for the integration of common biometric technologies throughout the Department of Defense.

5.6. The Chairman of the Joint Chiefs of Staff shall:

5.6.1. Serve as the principal military advisor to the Secretary of Defense on IA.

5.6.2. Ensure, in coordination with the ASD(*NI*), the validation of IA requirements for systems supporting Joint and Combined operations through the Joint Requirements Oversight Council.

5.6.3. Develop, coordinate, and promulgate IA policies, doctrine and procedures for Joint and Combined operations.

5.7. The Commander, United States Strategic Command, shall coordinate and direct DoD-wide CND operations in accordance with reference (m).

5.8. The Director, National Security Agency (NSA), shall:

5.8.1. Implement an IA intelligence capability responsive to requirements for the Department of Defense, less DIA responsibilities.

5.8.2. Provide IA support to the DoD Components as required in order to assess the threats to, and vulnerabilities of, information technologies.



5.8.3. Serve as the DoD focal point for IA cryptographic research and development in accordance with DDR&E direction and in coordination with the Director, DARPA.

5.8.4. Manage the development of the IA Technical Framework (reference (a)) in support of defense-in-depth, and provide engineering support and other technical assistance for its implementation within the Department of Defense.

5.8.5. Serve as the DoD focal point for the NIAP and establish criteria and processes for evaluating and validating all IA and IA-enabled IT products used in DoD information systems.

5.8.6. Plan, design, and manage the implementation of the Key Management Infrastructure/PKI within the Department of Defense.

5.8.7. In coordination with the USD(AT&L), develop and maintain an information system security engineering process that supports IT acquisition.

5.8.8. Support the Director, Defense Information Systems Agency in the development of security configuration guidance for IA and IA-enabled IT products.

5.8.9. Develop, implement, and oversee an IA program for layered protection of DoD cryptologic SCI systems, an IA certification and accreditation process for DoD cryptologic SCI applications, enclaves, platform IT interconnections and outsourced IT-based processes, and an IA education, training, and awareness program for users and administrators of DoD cryptologic SCI systems.

5.9. The Director, Operational Testing and Evaluation, shall oversee IA assessments.

5.10. The Heads of the DoD Components shall:

5.10.1. Develop and implement an IA program focused on assurance of DoD Component-specific information and systems (e.g., sustaining base, tactical, and Command, Control, Communications, Computers, and Intelligence (C4I) interfaces to weapon systems) that is consistent with references (a) and (l) and defense-in-depth.

5.10.2. Coordinate with Joint and Defense-wide program offices to ensure interoperability of IA solutions across the DoD enterprise.

5.10.3. Collect and report IA management, financial, and readiness data to meet DoD IA internal and external reporting requirements.

5.10.4. Appoint DAAs for all DoD information systems for which they have responsibility.

5.10.5. Identify and include IA requirements in the design, acquisition, installation, operation, upgrade or replacement of all DoD information systems for which they have responsibility.

5.10.6. Ensure that the Government's contract requirements properly reflect that IA or IA-enabled IT products are involved and must be properly evaluated and validated in accordance with paragraph 4.17., above.


5.10.7. Ensure that IA awareness, training, education, and professionalization are provided to all Component personnel commensurate with their respective responsibilities for developing, using, operating, administering, maintaining, and retiring DoD information systems.

5.10.8. Comply with established accreditation and connection approval processes required for all DoD information systems.

5.10.9. Coordinate all IA research and technology initiatives under their purview with the DDR&E.

## 6. EFFECTIVE DATE

This Directive is effective immediately.



Paul Wolfowitz  
Deputy Secretary of Defense

Enclosures - 2

E1. References, continued

E2. Definitions

E1. ENCLOSURE 1

REFERENCES, continued

- (e) DoD CIO Memorandum 6-8510, "Guidance and Policy for Department of Defense Global Information Grid Information Assurance," June 16, 2000 (hereby canceled)
- (f) DoD 5025.1-M, "DoD Directives System Procedures," *March 5, 2003*
- (g) Executive Order 12333, "United States Intelligence Activities," December 4, 1981
- (h) DoD Directive *5144.1, "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005*
- (i) National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009, "National Information Systems Security Glossary," September 2000<sup>2</sup>
- (j) OMB Circular A-130, "Management of Federal Information Resources, Transmittal 4," November 30, 2000
- (k) DoD Directive 5000.1, "The Defense Acquisition System," *May 12, 2003*
- (l) Sections 1423 and 1451 of title 40, United States Code, "Division E of the Clinger-Cohen Act of 1996"
- (m) DoD Directive O-8530.1, "Computer Network Defense," January 8, 2001
- (n) DoD 5200.2-R, "DoD Personnel Security Program," *December 16, 1986*
- (o) DoD 5200.1-R, "DoD Information Security Program Regulation," January 14, 1997
- (p) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992
- (q) DoD Directive 5230.20E, "Visits *and* Assignments of Foreign Nationals," *June 22, 2005*
- (r) DoD Instruction 5230.27, "Presentation of DoD-Related Scientific and Technical Papers at Meetings," October 6, 1987
- (s) DoD Directive 5230.9, "Clearance of DoD Information for Public Release," April 9, 1996
- (t) DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," August 6, 1999
- (u) DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation (C&A) Process (DITSCAP)," December 30, 1997
- (v) DoD Directive C-5200.5, "Communications Security (COMSEC)," (U) April 21, 1990
- (w) National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, "National Policy Governing the Acquisition of Information Assurance (IA) and IA-enabled Information Technology Products," January 2000
- (x) DoD Directive *3020.40, "Defense Critical Infrastructure Program (DCIP)," August 19, 2005*
- (y) DoD 5220.22-M, "National Industrial Security Program Operating Manual," January 1995 and "National Industrial Security Program Operating Manual Supplement," February 1995

<sup>2</sup> Available at <http://www.nstissc.gov/html/library.html>

- (z) Title 48, Code of Federal Regulations, "Federal Acquisition Regulations System," October 1, 1996<sup>3</sup>
- (a*a*) Information Assurance Technical Framework (IATF), Release 3.0, September 2000<sup>4</sup>
- (a*b*) DoD 7000.14-R, Vol 2B, Chapter 5, "DoD Financial Management Regulation," June 2000
- (a*c*) Section 552a of title 5, United States Code, "The Privacy Act of 1974"
- (a*d*) Section 278g-3 of title 15, United States Code, "Computer Security Act of 1987"
- (a*e*) DoD 5400.7-R, "DoD Freedom of Information Act Program," September 4, 1998
- (a*f*) Section 552 of title 5, United States Code, "Freedom of Information Act"
- (a*g*) DoD Directive 5210.83, "Department of Defense Unclassified Controlled Nuclear Information (DoD UCNI)", November 15, 1991
- (a*h*) DoD Directive 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure," November 6, 1984

<sup>3</sup> Available at <http://web1.deskbook.osd.mil/htmlfiles/rlcats.asp>

<sup>4</sup> Available at <http://www.iatf.net>

## E2. ENCLOSURE 2

### DEFINITIONS

E2.1.1. Application. Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring or administrative privileges. Examples include office automation, electronic mail, web services, and major functional or mission software programs.

E2.1.2. Authentication. Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information (reference (i)).

E2.1.3. Authorized User. Any appropriately cleared individual with a requirement to access a DoD information system in order to perform or assist in a lawful and authorized governmental function.

E2.1.4. Availability. Timely, reliable access to data and information services for authorized users (reference (i)).

E2.1.5. Community Risk. Probability that a particular vulnerability will be exploited within an interacting population and adversely impact some members of that population.

E2.1.6. Computer Network. The constituent element of an enclave responsible for connecting computing environments by providing short-haul data transport capabilities such as local or campus area networks, or long-haul data transport capabilities such as operational, metropolitan, or wide area and backbone networks.

E2.1.7. Computing Environment. Workstation or server (host) and its operating system, peripherals, and applications (reference (i)).

E2.1.8. Confidentiality. Assurance that information is not disclosed to unauthorized entities or processes (reference (i)).

E2.1.9. Connection Approval. Formal authorization to interconnect information systems.

E2.1.10. Controlled Unclassified Information. A term used, but not specifically defined in reference (o), to refer to sensitive information as defined in paragraph E2.1.41., below.

E2.1.11. Defense-in-Depth. The DoD approach for establishing an adequate IA posture in a shared-risk environment that allows for shared mitigation through: the integration of people, technology, and operations; the layering of IA solutions within and among IT assets; and, the selection of IA solutions based on their relative level of robustness.

E2.1.12. Defense Information System Network (DISN). The DoD consolidated worldwide enterprise-level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations.

E2.1.13. Designated Approving Authority (DAA). The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with Designated Accrediting Authority and Delegated Accrediting Authority (reference (i)).

E2.1.14. DISN Designated Approving Authority (DISN DAA). One of four DAAs responsible for operating the DISN at an acceptable level of risk. The four DISN DAAs are the Directors of the DISA, the DIA, the NSA and the Director of the Joint Staff (delegated to the Joint Staff Director for Command, Control, Communications, and Computer Systems (J-6)).

E2.1.15. DMZ (Demilitarized Zone). Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's IA policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal network from outside attacks. A DMZ is also called a "screened subnet."

E2.1.16. DoD Information System. Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes AIS applications, enclaves, outsourced IT-based processes, and platform IT interconnections.

E2.1.16.1. Automated Information System (AIS) Application. For DoD information assurance purposes, an AIS application is the product or deliverable of an acquisition program, such as those described in reference (k). An AIS application performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed as part of the acquisition. An AIS application may be a single software application (e.g., Integrated Consumable Items Support); multiple software applications that are related to a single mission (e.g., payroll or personnel); or a combination of software and hardware performing a specific support function across a range of missions (e.g., Global Command and Control System, Defense

Messaging System). AIS applications are deployed to enclaves for operations, and have their operational security needs assumed by the enclave. Note that an AIS application is analogous to a "major application" as defined in reference (j); however, this term is not used in order to avoid confusion with the DoD acquisition category of Major Automated Information System.

E2.1.16.2. Enclave. Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves always assume the highest mission assurance category and security classification of the AIS applications or outsourced IT-based processes they support, and derive their security needs from those systems. They provide standard IA capabilities such as boundary defense, incident detection and response, and key management, and also deliver common applications such as office automation and electronic mail. Enclaves are analogous to general support systems as defined in reference (j). Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers.

E2.1.16.3. Outsourced IT-based Process. For DoD IA purposes, an outsourced IT-based process is a general term used to refer to outsourced business processes supported by private sector information systems, outsourced information technologies, or outsourced information services. An outsourced IT-based process performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed in both acquisition and operations.

E2.1.16.4. Platform IT Interconnection. For DoD IA purposes, platform IT interconnection refers to network access to platform IT. Platform IT interconnection has readily identifiable security considerations and needs that must be addressed in both acquisition, and operations. Platform IT refers to computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems such as weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems such as water and electric. Examples of platform IT interconnections that impose security considerations include communications interfaces for data exchanges with enclaves for mission planning or execution, remote administration, and remote upgrade or reconfiguration.

E2.1.17. Information Assurance (IA). Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

E2.1.18. IA Certification and Accreditation. The standard DoD approach for identifying information security requirements, providing security solutions, and managing the security of DoD information systems.

E2.1.19. IA Control. An objective IA condition of integrity, availability or confidentiality achieved through the application of specific safeguards or through the regulation of specific activities that is expressed in a specified format, i.e., a control number, a control name, control text, and a control class. Specific management, personnel, operational, and technical controls are applied to each DoD information system to achieve an appropriate level of integrity, availability, and confidentiality in accordance with reference (j).

E2.1.20. IA Product. Product or technology whose primary purpose is to provide security services (e.g., confidentiality, authentication, integrity, access control, non-repudiation of data); correct known vulnerabilities; and/or provide layered defense against various categories of non-authorized or malicious penetrations of information systems or networks. Examples include such products as data/network encryptors, firewalls, and intrusion detection devices.

E2.1.21. IA-Enabled Information Technology Product. Product or technology whose primary role is not security, but which provides security services as an associated feature of its intended operating capabilities. Examples include such products as security-enabled web browsers, screening routers, trusted operating systems, and security-enabled messaging systems.

E2.1.22. Information Owner. Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

E2.1.23. Integrity. Quality of an information system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information (reference (i)).

E2.1.24. IT Position Category. Applicable to unclassified DoD information systems, a designator that indicates the level of IT access required to execute the responsibilities of the position based on the potential for an individual assigned to the position to adversely impact DoD missions or functions. Position categories include: IT-I (Privileged), IT-II (Limited Privileged) and IT-III (Non-Privileged), as defined in reference (o). Investigative requirements for each category vary, depending on role and whether the incumbent is a U.S. military member, U.S. civilian government employee, U.S. civilian contractor or a foreign national. The term IT Position is synonymous with the older term Automated Data Processing (ADP) Position.



E2.1.25. Mission Assurance Category (MAC). Applicable to DoD information systems, the mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. The Department of Defense has three defined mission assurance categories:

E2.1.25.1. Mission Assurance Category I (MAC I). Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures.

E2.1.25.2. Mission Assurance Category II (MAC II). Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure adequate assurance.

E2.1.25.3. Mission Assurance Category III (MAC III). Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques or procedures generally commensurate with commercial best practices.

E2.1.26. Mobile Code. Software modules obtained from remote systems, transferred across a network, and then downloaded and executed on local systems without explicit installation or execution by the recipient.

E2.1.27. National Information Assurance Partnership (NIAP). Joint initiative between the NSA and the National Institute of Standards and Technology responsible for security testing needs of both IT consumers and producers and promoting the development of technically sound security requirements for IT products and systems and appropriate measures for evaluating those products and systems.

E2.1.28. Need-to-Know. Necessity for access to, or knowledge or possession of, specific official DoD information required to carry out official duties (reference (i) modified).

E2.1.29. Need-to-Know Determination. Decision made by an authorized holder of official information that a prospective recipient requires access to specific official information to carry out official duties (reference (i)).

E2.1.30. Non-repudiation. Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data (reference (i)).

E2.1.31. Official DoD Information. All information that is in the custody and control of the Department of Defense, relates to information in the custody and control of the Department, or was acquired by DoD employees as part of their official duties or because of their official status within the Department (reference (s)).

E2.1.32. Portfolio. The aggregate of IT investments for DoD information systems, infrastructure and related technical activities that are linked to mission goals, strategies, and architectures, using various assessment and analysis tools to permit information and IT decisions to be based on their contribution to the effectiveness and efficiency of military missions and supporting business functions. Portfolios enable the Department of Defense to manage IT resources and align strategies and programs with Defense-wide, functional, and organizational goals and measures.

E2.1.33. Proxy. Software agent that performs a function or operation on behalf of another application or system while hiding the details involved. Typical proxies accept a connection from a user, make a decision as to whether or not the user or client network address is authorized to use the requested service, optionally perform additional authentication, and then complete a connection on behalf of the user to a remote destination.

E2.1.34. Public Domain Software. Software not protected by copyright laws of any nation that carries no warranties or liabilities, and may be freely used without permission of or payment to the creator.

E2.1.35. Public Information. Official DoD information that has been reviewed and approved for public release by the information owner in accordance with reference (s).

E2.1.36. Research and Technology. Activities that may be described as basic research, applied research, and advanced technology development, demonstrations or equivalent activities, regardless of budget activity. Definitions for Basic Research, Applied Research and Advanced Technology Development are provided in the DoD FMR, Chapter 5 (reference (a**b**)).

E2.1.37. Robustness. A characterization of the strength of a security function, mechanism, service or solution, and the assurance (or confidence) that it is implemented and functioning correctly. The Department of Defense has three levels of robustness:

E2.1.37.1. High Robustness: Security services and mechanisms that provide the most stringent protection and rigorous security countermeasures.

E2.1.37.2. Medium Robustness: Security services and mechanisms that provide for layering of additional safeguards above good commercial practices.

E2.1.37.3. Basic Robustness: Security services and mechanisms that equate to good commercial practices.

E2.1.38. Security Domain. Within an information system, the set of objects that is accessible. Access is determined by the controls associated with information properties such as its security classification, security compartment or sensitivity. The controls are applied both within the information system and in its connection to other classified or unclassified information systems.

E2.1.39. Sensitive But Unclassified (SBU). A term commonly and inappropriately used within the Department of Defense as a synonym for Sensitive Information, which is the preferred term.

E2.1.40. Sensitive Compartmented Information (SCI). Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence.

E2.1.41. Sensitive Information. Information the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of title 5, United States Code, "The Privacy Act" (reference (ac)), but which has not been specifically authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy (Section 278g-3 of title 15, United States Code, "The Computer Security Act of 1987" (reference (ad))). This includes information in routine DoD payroll, finance, logistics, and personnel management systems. Sensitive information sub-categories include, but are not limited to the following:

E2.1.41.1. For Official Use Only (FOUO). In accordance with DoD 5400.7-R (reference (ae)), DoD information exempted from mandatory public disclosure under the Freedom of Information Act (FOIA) (reference (af)).

E2.1.41.2. Privacy Data. Any record that is contained in a system of records, as defined in the reference (ac) and information the disclosure of which would constitute an unwarranted invasion of personal privacy.

E2.1.41.3. DoD Unclassified Controlled Nuclear Information (DoD UCNI). Unclassified information on security measures (security plans, procedures and equipment) for the physical protection of DoD Special Nuclear Material (SNM), equipment, or facilities in accordance with DoD Directive 5210.83 (reference (ag)). Information is Designated DoD UCNI when it is determined that its unauthorized disclosure could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by increasing significantly the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of DoD SNM, equipment, or facilities.

E2.1.41.4. Unclassified Technical Data. Data that is not classified, but is subject to export control and is withheld from public disclosure according to DoD Directive 5230.25 (reference (ah)).

E2.1.41.5. Proprietary. Information that is provided by a source or sources under the condition that it not be released to other sources.

E2.1.41.6. Foreign Government Information. Information that originated from a foreign government and that is not classified CONFIDENTIAL or higher, but must be protected in accordance with reference (o).

E2.1.41.7. Department of State Sensitive But Unclassified (DoS SBU). Information which originated from the DoS that has been determined to be SBU under appropriate DoS information security policies.

E2.1.41.8. Drug Enforcement Administration (DEA) Sensitive Information. Information originated by the DEA that requires protection against unauthorized disclosure to protect sources and methods of investigative activity, evidence, and the integrity of pretrial investigative reports.

E2.1.42. Supporting IA Infrastructures. Collections of interrelated processes, systems, and networks that provide a continual flow of information assurance services throughout the Department of Defense, e.g., the key management infrastructure or the incident detection and response infrastructure.

E2.1.43. Telework. Any arrangement in which an employee performs officially assigned duties at an alternative worksite on either a regular and recurring, or on an ad hoc, basis (not including while on official travel).



**DoD 8570.01-M**

# **Information Assurance Workforce Improvement Program**

*Incorporating Change 3,  
January 24, 2012*

**December 19, 2005  
Assistant Secretary of Defense for  
Networks and Information  
Integration/Department of Defense Chief  
Information Officer**

**[Use appropriate letterhead]**

December 19, 2005

## FOREWORD

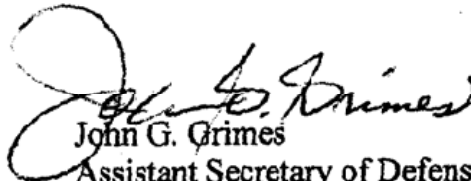
This Manual is issued under the authority of DoD Directive 8570.1 “Information Assurance Training, Certification, and Workforce Management,” August 15, 2004 (Reference (a)). It provides guidance and procedures for the training, certification, and management of the DoD workforce conducting Information Assurance (IA) functions in assigned duty positions. It also provides information and guidance on reporting metrics and the implementation schedule for Reference (a).

This Manual applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the “DoD Components”).

This Manual is effective immediately and is mandatory for use by all the DoD Components. Send recommended changes to the Manual to the following address:

Deputy Assistant Secretary of Defense for Information and Identity Assurance  
Assistant Secretary of Defense for Network and Information Integration/Department of  
Defense Chief Information Officer (ASD(NII)/DoD CIO)  
1155 Defense Pentagon  
Washington, DC 20301-1155

The DoD Components, other Federal agencies, and the public may download this Manual from the DoD Issuances Web Site at <http://www.dtic.mil/whs/directives>.



John G. Grimes  
Assistant Secretary of Defense for  
Networks and Information Integration/  
DoD Chief Information Officer

TABLE OF CONTENTS

	<u>Page</u>
FOREWORD	2
TABLE OF CONTENTS	3
FIGURES	6
TABLES	6
REFERENCES	7
ACRONYMS	9
CHAPTER 1 – GENERAL INFORMATION	12
C1.1. PURPOSE	12
C1.2. DEFINITIONS	12
C1.3. DoD IA WORKFORCE MANAGEMENT OBJECTIVES	12
C1.4. RESPONSIBILITIES	13
CHAPTER 2 – IA WORKFORCE STRUCTURE OVERVIEW	17
C2.1. INTRODUCTION	17
C2.2. IA WORKFORCE CATEGORIES, SPECIALTIES, AND LEVELS	18
C2.3. TRAINING AND CERTIFICATION PROGRAMS	19
CHAPTER 3 – IA WORKFORCE TECHNICAL CATEGORY	21
C3.1. INTRODUCTION	21
C3.2. TECHNICAL CATEGORY DESCRIPTION	21
C3.3. INFORMATION ASSURANCE TECHNICAL LEVEL I	25
C3.4. INFORMATION ASSURANCE TECHNICAL LEVEL II	267
C3.5. INFORMATION ASSURANCE TECHNICAL LEVEL III	29
CHAPTER 4 – IA WORKFORCE MANAGEMENT CATEGORY	32
C4.1. INTRODUCTION	32
C4.2. MANAGEMENT CATEGORY DESCRIPTION	32
C4.3. INFORMATION ASSURANCE MANAGEMENT LEVEL I	34
C4.4. INFORMATION ASSURANCE MANAGEMENT LEVEL II	36
C4.5. INFORMATION ASSURANCE MANAGEMENT LEVEL III	38
CHAPTER 5 – DESIGNATED ACCREDITING AUTHORITY (DAA)	
REQUIREMENTS	41
C5.1. INTRODUCTION	41
C5.2. DAA FUNCTIONS AND RESPONSIBILITIES	41

C5.3. DAA TRAINING AND CERTIFICATION REQUIREMENT	42
CHAPTER 6 – AUTHORIZED USER MINIMUM IA AWARENESS REQUIREMENTS	44
C6.1. INTRODUCTION	44
C6.2. GENERAL REQUIREMENTS	44
C6.3. SPECIFIC REQUIREMENTS	45
CHAPTER 7 – IA WORKFORCE IDENTIFICATION, TRACKING, AND ASSIGNMENT	48
C7.1. INTRODUCTION	48
C7.2. IA WORKFORCE MANAGEMENT	48
C7.3. IA WORKFORCE IDENTIFICATION REQUIREMENTS	49
CHAPTER 8 – IA WORKFORCE MANAGEMENT REPORTING AND METRICS	52
C8.1. INTRODUCTION	52
C8.2. REPORTING- <i>IA WORKFORCE METRICS</i> REQUIREMENTS	52
CHAPTER 9 – IA WORKFORCE IMPLEMENTATION REQUIREMENTS	58
C9.1. INTRODUCTION	58
C9.2. GENERAL REQUIREMENTS	58
C9.3. SPECIFIC REQUIREMENTS	58
C9.4. IMPLEMENTATION PLAN REPORTING REQUIREMENTS	60
CHAPTER 10 – IA WORKFORCE SYSTEM ARCHITECTURE AND ENGINEERING (IASAE) SPECIALTY	61
C10.1. INTRODUCTION	61
C10.2. IASAE SPECIALTY DESCRIPTION	61
C10.3. IASAE LEVEL I	63
C10.4. IASAE LEVEL II	66
C10.5. IASAE LEVEL III	69
CHAPTER 11 – COMPUTER NETWORK DEFENSE-SERVICE PROVIDER (CND-SP) SPECIALTY	73
C11.1. INTRODUCTION	73
C11.2. ACCREDITED CND-SP SPECIALTY DESCRIPTION	73
C11.3. COMPUTER NETWORK DEFENSE ANALYST	76
C11.4. COMPUTER NETWORK DEFENSE INFRASTRUCTURE SUPPORT	77
C11.5. COMPUTER NETWORK DEFENSE INCIDENT RESPONDER	798
C11.6. COMPUTER NETWORK DEFENSE AUDITOR	80
C11.7. COMPUTER NETWORK DEFENSE SERVICE PROVIDER MANAGER	81



APPENDICES

AP1. Appendix 1, DEFINITIONS	83
AP2. Appendix 2, IA WORKFORCE LEVELS, FUNCTIONS AND CERTIFICATION APPROVAL PROCESS	89
AP3. Appendix 3, IA WORKFORCE REQUIREMENTS AND CERTIFICATIONS	91
AP4. Appendix 4, SAMPLE STATEMENT OF ACCEPTANCE OF RESPONSIBILITIES	956

FIGURES

Figure C2.F1. Overview of Basic IA Workforce Structure	19
Figure C5.F1. Sample DAA Certificate of Completion	43
Figure C8.F1. IA WIP Annual Report Format <i>and Workforce Management Metrics</i>	56
<del>Figure C9.F1. IA Workforce Milestone Budget Plan Report</del>	<del>60</del>

TABLES

Table C3.T1. IA Technical Workforce Requirements	24
Table C3.T2. IA Technical Level I Position Requirements	25
Table C3.T3. IA Technical Level I Functions	25
Table C3.T4. IA Technical Level II Position Requirements	27
Table C3.T5. IA Technical Level II Functions	27
Table C3.T6. IA Technical Level III Position Requirements	29
Table C3.T7. IA Technical Level III Functions	30
Table C4.T1. IA Management Workforce Requirements	32
Table C4.T2. IA Management Level I Position Requirements	34
Table C4.T3. IA Management Level I Functions	35
Table C4.T4. IA Management Level II Position Requirements	36
Table C4.T5. IA Management Level II Functions	37
Table C4.T6. IA Management Level III Position Requirements	38
Table C4.T7. IA Management Level III Functions	39
Table C5.T1. DAA Functions	42
Table C10.T1. IASAE Workforce Requirements	61
Table C10.T2. IASAE Level I Position Requirements	63
Table C10.T3. IASAE Level I Functions	64
Table C10.T4. IASAE Level II Position Requirements	66
Table C10.T5. IASAE Level II Functions	67
Table C10.T6. IASAE Level III Position Requirements	69
Table C10.T7. IASAE Level III Functions	70
Table C11.T1. Accredited CND-SP Workforce Requirements	75
Table C11.T2. CND Analyst Position Requirements	76
Table C11.T3. CND Analyst Functions	77
Table C11.T4. CND Infrastructure Support Position Requirements	77
Table C11.T5. CND Infrastructure Support Functions	78
Table C11.T6. CND Incident Responder Position Requirements	79
Table C11.T7. CND Incident Responder Functions	79
Table C11.T8. CND Auditor Position Requirements	80
Table C11.T9. CND Auditor Functions	81
Table C11.T10. CND Service Provider Manager Position Requirements	81
Table C11.T11. CND Service Provider Manager Functions	82
Table AP3.T1. Summary of IA Workforce Requirements	91
<del>Table AP3.T2. DoD Approved Baseline Certifications</del>	<del>92</del>
<del>Table AP3.T3. IA Workforce Certification Organizations</del>	<del>93</del>

## REFERENCES

- (a) DoD Directive 8570.1, “Information Assurance Training, Certification, and Workforce Management,” August 15, 2004
- (b) DoD Instruction 8500.2, “Information Assurance (IA) Implementation,” February 6, 2003
- (c) Section 3544 of title 44 United States Code
- (~~d~~) *DoD Instruction 5105.18, “DoD Intergovernmental and Intragovernmental Committee Management Program,” July 10, 2009*
- (~~de~~) Title 29, Code of Federal Regulations, section 1607, current edition
- (~~ef~~) Office of Personnel Management Job Family Position Classification Standard for Administrative Work in the Information Technology Group, GS-2200; Information Technology Management, GS-2210, May 2001, as revised<sup>1</sup>
- (~~zg~~) DoD 1400.25-M Subchapter 1920, “Classification,” April 28, 2006
- (~~fh~~) DoD Directive 8500.1, “Information Assurance (IA),” October 24, 2002
- (~~gi~~) DoD Directive O-8530.1, “Computer Network Defense (CND),” January 8, 2001
- (~~hj~~) DoD 5200.2-R, “Personnel Security Program,” January 1987
- (~~ik~~) DoD Instruction 8510.01, “DoD Information Assurance Certification and Accreditation Process (DIACAP),” November 28, 2007
- (~~jl~~) Section 2224 of title 10, United States Code. “Defense Information Assurance Program”
- (~~km~~) Section 278g-3 of title 15, United States Code
- (~~ln~~) Office of Management and Budget Circular A-130, “Management of Federal Information Resources, Transmittal Memorandum No. 4,” Appendix 3, November 30, 2000
- (~~mo~~) Department of Homeland Security National Cyber Security Division Program Management Office, “Customer Agency Guide Information Systems Security Line of Business (ISS LOB), Shared Service Centers for Tier 1 Security Awareness Training and FISMA Reporting,” February 27, 2007
- (~~np~~) DoD Directive 1000.25, “DoD Personnel Identity Protection (PIP) Program,” July 19, 2004
- (~~oq~~) DoD Instruction 7730.64, “Automated Extracts of Manpower and Unit Organizational Element Files,” December 11, 2004
- (~~pr~~) DoD Instruction 1336.5, “Automated Extract of Active Duty Military Personnel Records,” May 2, 2001
- (~~qs~~) DoD Instruction 7730.54, “Reserve DoD Components Common Personnel Data System (RCCPDS),” August 6, 2004
- (~~rt~~) DoD Instruction 1444.2, “Consolidation of Automated Civilian Personnel Records,” September 16, 1987
- (~~su~~) DoD 8910.1-M, “DoD Procedures for Management of Information Requirements,” June 30, 1998
- (~~tv~~) Director of Central Intelligence Directive 6/3, “Protecting Sensitive Compartmented Information within Information Systems,” June 5, 1999
- (~~uw~~) Committee on National Security Systems Instruction No. 4009, “National Information Security System Glossary,” as revised May 2003

---

<sup>1</sup> www.opm.gov/fedclass/gs2200a.pdf

- (~~v~~x) Joint Publication 1-02, “Department of Defense Dictionary of Military and Associated Terms,” as amended
- (~~w~~y) Chapter 51 of title 5, United States Code
- (~~x~~z) International Standards Organization/International Electronics Commission (ISO/IEC) 17024, “General Requirements for Bodies Operating Certification of Persons,” April 2003
- (~~y~~aa) DoD 5500.7-R, “DoD Joint Ethics Regulation,” August 1, 1993

ACRONYMS

<b>Acronym</b>	<b>Meaning</b>
ASD(NII)/DoD CIO	Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer
C&A	Certification and Accreditation
CBT	Computer Based Training
CDS	Cross Domain Solutions
CE	Computing Environment
CIO	Chief Information Officer
CO/XO	Commanding Officer/Executive Officer
CND	Computer Network Defense
CND-A	Computer Network Defense Analyst
CND-AU	Computer Network Defense Auditor
CND-IS	Computer Network Defense Infrastructure Support
CND-IR	Computer Network Defense Incident Responder
CND-SP	Computer Network Defense Service Provider
CND-SPM	Computer Network Defense Service Provider Manager
COOP	Continuity of Operations Plan
CUI	Controlled Unclassified Information
DAA	Designated Accrediting Authority
DCIO	Deputy Chief Information Officer
DCPDS	Defense Civilian Personnel Data System
DEERS	Defense Eligibility Enrollment Reporting System
<del>DHS LoB</del>	<del>Department of Homeland Security Line of Business</del>
DIAP	Defense-wide Information Assurance Program
DISA	Defense Information Systems Agency
DMDC	Defense Manpower Data Center
DoD	Department of Defense
DWCA	Defense Workforce Certification Application

<b>Acronym</b>	<b>Meaning</b>
e-JMAPS	e-Joint Manpower and Personnel System
FISMA	Federal Information Security Management Act
FN	Foreign National
FY	Fiscal Year
GIG	Global Information Grid
GS	General Schedule
IA	Information Assurance
IAM	Information Assurance Management
IAO	Information Assurance Officer
IASE	Information Assurance Support Environment (DoD IA Portal)
IASAE	Information Assurance System Architect and Engineer
IAT	Information Assurance Technical
IAVA	Information Assurance Vulnerability Alert
IAVB	Information Assurance Vulnerability Bulletin
IAVM	Information Assurance Vulnerability Management
IA WIPAC	Information Assurance Workforce Improvement Program Advisory Council
INFOSEC	“Security” (The parenthetical title in DCPDS for civilian personnel performing security (IA) functions)
IRT	Incident Response Teams
IS	Information System
(ISC)2	International Information Systems Security Certification Consortium
ISO/IEC	International Organization for Standardization /International Electro-technical Commission
ISS LoB	Information System Security Line of Business
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology

<b>Acronym</b>	<b>Meaning</b>
LN	Local National
MAC	Mission Assurance Category
NE	Network Environment
NIPRNet	Non-classified Internet Protocol Router Network
<del>NSPS</del>	<del>National Security Personnel System</del>
OJT	On the Job Training
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OSD	Office of the Secretary of Defense
PSC	Position Specialty Code
SCI	Sensitive Compartmented Information
SIPRNet	Secret Internet Protocol Router Network
SP	Service Provider
SSC	Shared Service Center
TA	Technical Advisory
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary of Defense for Intelligence
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USSTRATCOM	United States Strategic Command
WIP	Workforce Improvement Program

## C1. CHAPTER 1

### GENERAL INFORMATION

#### C1.1. PURPOSE

This Manual:

C1.1.1. Implements DoD Directive 8570.1 (Reference (a)).

C1.1.2. Provides guidance for the identification and categorization of positions and certification of personnel conducting Information Assurance (IA) functions within the DoD workforce supporting the DoD Global Information Grid (GIG) per DoD Instruction 8500.2 (Reference (b)). The DoD IA Workforce includes, but is not limited to, all individuals performing any of the IA functions described in this Manual. Additional chapters focusing on personnel performing specialized IA functions including certification and accreditation (C&A) and vulnerability assessment will be published as changes to this Manual.

C1.1.3. Establishes IA workforce ~~oversight and~~ management reporting requirements to support Reference (a).

C1.2. DEFINITIONS. See Appendix 1.

#### C1.3. DoD IA WORKFORCE MANAGEMENT OBJECTIVES:

C1.3.1. Develop a DoD IA workforce with a common understanding of the concepts, principles, and applications of IA for each category, specialty, level, and function to enhance protection and availability of DoD information, information systems, and networks.

C1.3.2. Establish baseline technical and management IA skills among personnel performing IA functions across the DoD enterprise.

C1.3.3. Provide warfighters qualified IA personnel in each category, specialty and level.

C1.3.4. Implement a formal IA workforce skill development and sustainment process, comprised of resident courses, distributive training, blended training, supervised on the job training (OJT), exercises, and certification/recertification.

C1.3.5. Verify IA workforce knowledge and skills through standard certification testing.

C1.3.6. Augment and expand on a continuous basis the knowledge and skills obtained through experience or formal education.



## C1.4. RESPONSIBILITIES

In addition to the responsibilities listed in Reference (a) and section 3544 of title 44, United States Code (Reference (c)), this Manual assigns the following:

C1.4.1. The Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO) shall:

C1.4.1.1. Coordinate changes and updates to this Manual to maintain state of the art functional and certification requirements for the IA workforce.

C1.4.1.2. Develop, coordinate, and publish baseline certification requirements for personnel performing specialized IA functions.

C1.4.1.3. Coordinate the implementation and sustainment requirements of this Manual to include supporting tools and resources (e.g., conferences, website, database integration, workforce identification).

C1.4.1.4. *Per DoD Instruction 5105.18 (Reference (d)) and* in coordination with the Under Secretary of Defense for Personnel and Readiness (USD(P&R)), *establish* an IA Workforce Improvement Program Advisory Council (IA WIPAC), to ensure that the requirements of Reference (a) and this Manual are met. The IA WIPAC shall:

C1.4.1.4.1. Meet at least annually at the call of the DoD Deputy Chief Information Officer (DCIO). At a minimum, its composition will include representatives from the Chairman of the Joint Chiefs of Staff; USD(P&R); the Under Secretary of Defense for Intelligence (USD(I)); the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)); the Military Departments and Services; the Defense Information Systems Agency (DISA); and the U.S. Strategic Command (USSTRATCOM). Members must be ~~government employees~~ *full-time or permanent part-time Federal employees or active-duty military members*.

C1.4.1.4.2. Establish an approval process for IA *baseline* certifications to be added to or deleted from the ~~Certification Table (AP3-T2)~~ *approved IA baseline certification list on the DISA IA Support Environment (IASE) website*. Certifications must have a strong correlation to IA workforce levels and functions. *The Defense-wide Information Assurance Program (DIAP) office will provide oversight to the IA WIPAC and IA baseline certification approval process outlined in AP2.2 and post updates to the DISA IASE website. The IA WIPAC Executive Secretariat will publish a memorandum to announce updates to the Certification Table.*

C1.4.1.4.3. Review and update the IA levels, functions, and associated certification requirements contained in this Manual.

C1.4.1.4.4. Monitor the DoD IA certification program process improvements.

C1.4.1.4.5. Review DoD Component programs and plans to validate/approve compliance with DoD baseline IA workforce management requirements. Reviews will include the following:

C1.4.1.4.5.1. DoD Component implementation and sustainment plans for IA workforce identification, training, certification, management, metrics, and documentation requirements as established in this Manual and References (a) and (c).

C1.4.1.4.5.2. DoD Component plans and methodologies to track, monitor, and document completion of IA Awareness training requirements for all network users as established in this Manual and References (a) and (c).

C1.4.1.4.6. Report recommended actions to the ASD(NII)/DoD CIO and the USD(P&R) based on these reviews or other information available to it (such as Federal Information Security Management Act (FISMA) Reporting Information or ~~reports~~ *metrics* required by this Manual) to improve the program.

C1.4.1.4.7. Conduct assessments to ensure the validity of the IA workforce functions, training, and certification requirements per 29 CFR Volume 4, section 1607 (Reference (~~de~~)).

C1.4.1.4.8. Prioritize enterprise-wide requirements for the development of training content to address gaps and deficiencies.

C1.4.1.5. Prepare an IA Workforce Improvement Program (WIP) Annual Report.

C1.4.1.6. Require the Director of the Defense Information Systems Agency (DISA) to:

C1.4.1.6.1. Provide appropriate representation to the IA WIPAC.

C1.4.1.6.2. Coordinate with the ~~Defense-wide IA Program (DIAP)~~ Office, USD(AT&L), and the DoD Components IA WIP Office of Primary Responsibility Points of Contact (OPR POC) to develop and maintain online resources correlating DoD IA training products and classes to requirements defined in law, executive orders, and DoD issuances. Additionally, provide information correlating IA functions (Chapters 3, 4, 5, 10, and 11) to workforce categories, specialties, and levels to core IA training curriculum.

C1.4.1.6.3. Serve as the DoD Shared Service Center (SSC) for the Office of Management and Budget (OMB)-directed Information System Security Line of Business (ISS LoB) for Tier I Awareness training. See Chapter 6 for additional information/requirements.

C1.4.1.7. Require the DIAP to provide IA workforce management oversight and coordination for the requirements established in this Manual.

C1.4.2. The Under Secretary of Defense for Personnel and Readiness (USD(P&R)) shall support and provide appropriate representation to the IA WIPAC. The Defense Activity for

Non-Traditional Education Support (DANTES) will manage the certification testing process requirement for the Department.

C1.4.3. The Undersecretary of Defense for Intelligence shall provide appropriate representation to the IA WIPAC to represent the intelligence community.

C1.4.4. The Heads of the DoD Components shall:

C1.4.4.1. Comply with the responsibilities and requirements of Reference (a) and this Manual.

C1.4.4.2. Provide support for the continuous improvement of the IA workforce management processes and maintenance of requirements. Provide appropriate representation as required to the IA WIPAC.

C1.4.4.3. Provide for initial IA orientation and annual awareness training to all authorized users to ensure they know, understand, and can apply the IA requirements of their system(s) in accordance with Reference (a) (see Chapter 6).

C1.4.4.4. Per Reference (a), identify all positions performing information system management, specialized, or privileged access IA functions by category, specialty, and level as described in Chapters 3, 4, 5, 10, and 11 of this Manual. This applies to all positions with IA duties, whether performed as primary or additional/embedded duties (see Chapters 2, 3, 4, 5, 7, 10, and 11). This requirement applies to military and civilian positions including those staffed by local nationals (LNs).

C1.4.4.5. Identify all IA function requirements to be performed by contractors in their statement of work/contract including LNs. Ensure contractors are appropriately certified, and have the appropriate background investigation to perform those IA functions.

C1.4.4.6. Train, certify, and obtain the proper background investigation for all military and civilian personnel identified as part of the IA workforce to accomplish their IA duties (see Chapters 3, 4, 5, 10, and 11, and Appendices 2 and 3).

C1.4.4.6.1. Include requirements for IA training in all DoD Component and local policy and procedures as part of the IA program.

C1.4.4.6.2. Ensure IA personnel performing IA functions obtain/maintain a certification corresponding to the highest level function(s) required by their position.

C1.4.4.6.3. Nominate, as appropriate, other certifications that correspond to the IA functions established for a particular level. Nominations may include operating system certifications that include the appropriate IA requirements. Provide nominations to the IA WIPAC.

C1.4.4.6.4. Obtain the appropriate background investigation per Reference (b) prior to granting unsupervised privileged access or management responsibilities to any DoD system.

C1.4.4.7. Identify, track, and monitor IA personnel performing IA functions (as described in Chapters 3, 4, 5, 10, and 11) to ensure that IA positions are staffed with trained and certified personnel (see Chapter 7).

C1.4.4.8. Collect metrics and submit reports to the ASD(NII)/DoD CIO to support planning and analysis of the IA workforce and annual FISMA reporting according to Reference (c) (see Chapter 8).

C1.4.4.9. Establish, resource, and implement plans, policies, and processes to meet the requirements of Reference (a) and this Manual (see Chapter 9).

C1.4.4.10. Identify all GS-2210 and other civilian positions/personnel (e.g., 0854, 1550) using the Office of Personnel Management (OPM) ~~or National Security Personnel System (NSPS)~~ specified parenthetical specialty titles per OPM Job Classification Standard (References ~~ef~~ and ~~zg~~). Enter the appropriate parenthetical specialty title for the primary function and may enter another specialty to identify additional duty responsibilities in the Defense Civilian Personnel Data System (DCPDS) or equivalent civilian personnel database. This is required for all DoD personnel even if the individual performs more than two specialties.

C1.4.4.11. Enter “INFOSEC” as the “Position Specialty Code” into the DCPDS in accordance with Reference (a) for 2210 and other civilian personnel (e.g., 0854, 1550) performing IA functions described in Chapters 3, 4, 5, 10, and 11 as primary, additional, or embedded duty and their category, specialty and level.

C1.4.4.12. Ensure that all DoD contracts requiring performance of IA functions (specified in Chapters 3, 4, 10, and 11) include the requirement to report contractor personnel’s IA certification status and compliance with this Manual. Contractors also must meet the background investigation requirements of Reference (b).

C1.4.4.13. Ensure personnel performing IA functions on national security systems meet the Committee on National Security Systems training requirements. This is in addition to the requirements of this Manual.

C1.4.4.14. Include appropriate IA content in officer accession programs, Flag, Commanding/Executive Officer (CO/XO), and Warrant Officer indoctrination, and DoD Component professional military education. The training is intended to develop leadership understanding of the critical importance of information assurance to the successful execution of DoD’s mission at all levels of the Department of Defense.

## C2. CHAPTER 2

### IA WORKFORCE STRUCTURE OVERVIEW

#### C2.1. INTRODUCTION

C2.1.1. IA functions focus on the development, operation, management, and enforcement of security capabilities for systems and networks. Personnel performing IA functions establish IA policies and implement security measures and procedures for the Department of Defense and affiliated information systems and networks.

C2.1.2. IA measures protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for their restoration by incorporating protection, detection, and reaction capabilities.

C2.1.3. IA duties may be performed as primary or additional/embedded duties, by a DoD employee (civilian, including LNs, or military) or by a support contractor (including LNs).

C2.1.4. As a condition of privileged access to any information system, personnel performing IA functions described in this Manual must satisfy both preparatory and sustaining DoD IA training and certification requirements (see Chapters 3, 4, 5, 10, and 11). Additionally, personnel with privileged access must complete a "Privileged Access Agreement," a sample of which is shown in Appendix 4, DoD Components may expand the requirements of this agreement to meet their needs.

C2.1.5. The certification requirements of this Manual apply to DoD civilian employees, military personnel, LNs, and support contractors performing the IA functions below and described in detail in Chapters 3, 4, 5, 10 and 11.

C2.1.6. Personnel performing IA duties addressed by Reference (a) and this Manual include the following IA oversight responsibilities:

C2.1.6.1. Work closely with data owners, information system owners, and users to ensure secure use and operation of information systems (IS) and networks.

C2.1.6.2. Ensure rigorous application of IA policies, principles, and practices in the delivery of all information technology (IT) services.

C2.1.6.3. Maintain system audit functions and periodically review audit information for detection of system abuses.

C2.1.6.4. Identify IA requirements as part of the IT acquisition development process.

C2.1.6.5. Assess and implement identified corrections (e.g., system patches and fixes) associated with technical vulnerabilities as part of the Information Assurance Vulnerability

Management (IAVM) program, consistent with References (a) and (b), DoD Directive 8500.1 (Reference (~~h~~)), and DoD Directive O-8530.1 (Reference (~~g~~)).

C2.1.6.6. Maintain configuration control of hardware, systems, and application software.

C2.1.6.7. Identify and properly react to security anomalies or integrity loopholes such as system weaknesses or vulnerabilities.

C2.1.6.8. Install and administer user identification or authentication mechanisms.

C2.1.7. The IA workforce training and certification program establishes a baseline of validated (tested) knowledge that is relevant, recognized, and accepted across the Department of Defense.

## C2.2. IA WORKFORCE CATEGORIES, SPECIALTIES, AND LEVELS

C2.2.1. This Manual identifies categories and specialties within the IA workforce. Categories are IA Technical (IAT) and IA Management (IAM). Specialties are Computer Network Defense Service Providers (CND-SPs) and IA System Architects and Engineers (IASAEs). These categories and specialties are subdivided into levels each based on functional skill requirements and/or system environment focus (see Chapters 3, 4, 5, 10, and 11).

C2.2.2. The levels and functions in the Technical, Management, CND-SP, and IASAE categories and specialties apply to civilian, military, and contractor personnel (including those LNs specifically authorized to perform IA functions according to Reference (b)).

C2.2.3. The levels and functions provide the basis to determine all IA Technical, IA Management, CND-SP, and IASAE staffing requirements. They also provide a framework for the identification of IAT, IAM, CND-SP and IASAE positions and qualified personnel (or those who can become qualified) across the Department of Defense.

C2.2.4. Each DoD position responsible for IA functional requirement(s) must be correlated with a category or specialty and level. Assigning position category or specialty levels based on functions across the Department of Defense establishes a common framework for identifying the IA workforce.

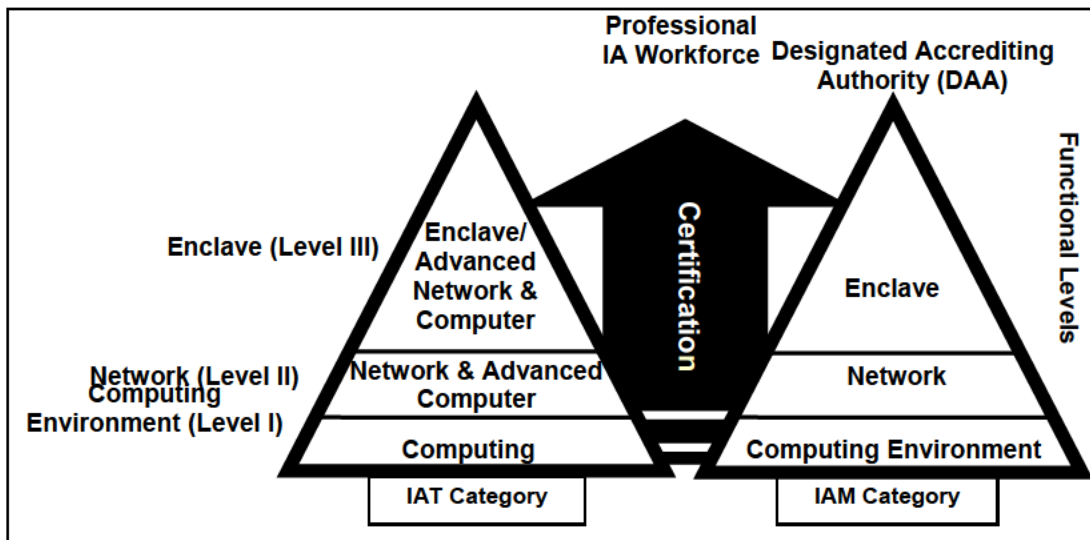
C2.2.5. A position may include functions spanning multiple levels. In these cases, the level, and related certification requirements will be those of the highest level functions. Individuals performing functions in multiple categories or specialties must hold certifications appropriate to the functions performed in each category or specialty. (Note: one certification may cover more than one category or specialty and level, (e.g., a Security + certification can qualify someone to fill both an IAT-I and an IAM-I position.)

C2.2.6. IA workforce categories or specialties and levels do not necessarily correlate to civilian grades, military ranks, or any specific occupational classification standard.



C2.2.7. Figure C2.F1., below, provides an overview of the basic IA workforce structure.

Figure C2.F1. Overview of Basic IA Workforce Structure



### C2.3. TRAINING AND CERTIFICATION PROGRAMS

C2.3.1. IA certification programs are intended to produce IA personnel with a baseline understanding of the fundamental IA principles and practices related to the functions of their assigned position. Each category, specialty, and skill level has specific training and certification requirements. Meeting these requirements will require a combination of formal training and experiential activities such as on-the-job training and continuing education. These training and certification requirements must be provided by the Department of Defense at no cost to government employees (military or civilian).

C2.3.2. The DoD Components must use certifications approved (and published ~~as part of this Manual~~ *on the DISA IASE website*) by the office of the ASD(NII)/DoD CIO ~~as to meet~~ the minimum *IA baseline* certification requirement.

C2.3.3. Approved certifications will demonstrate close correlation to the IA categories, specialties, levels, and functions described in Chapters 3, 4, 5, 10, and 11, and demonstrate portability throughout the Department of Defense, the Federal government, and the private sector.

C2.3.4. Individuals in IA positions, as defined in Chapters 3, 4, 5, 10, and 11 not meeting ~~certification~~ *qualification* requirements must be reassigned to other duties, consistent with applicable law. Until certification is attained, individuals in IA positions not meeting ~~certification~~ *qualification* requirements may perform those duties under the direct supervision of an appropriately certified individual unless the ~~certification~~ *qualification* requirement has been waived due to severe operational or personnel constraints. (See paragraphs C3.2.4.2., C3.2.4.3., C4.2.3.2.1., C4.2.3.4.2., C10.2.3.4., and C11.2.4.2.)

C2.3.5. Appendix 2 establishes the IA workforce certification requirement and criteria for assigned responsibilities. It also includes a requirement for the periodic review of DoD categories, specialties, functions, levels, and the approval of their associated certifications.

C2.3.6. Appendix 3 provides a matrix of ~~certifications~~ *qualifications* and the categories, specialties and levels to which they apply. IA workforce members must obtain *all* the ~~certification~~ *qualifications* corresponding to their IA functions as defined in Chapters 3, 4, 5, 10, and 11, and Appendix 3.

C2.3.7. Certification holders must adhere *to all recertification policies set by their certification provider and* ensure that their ~~certificates~~ *certifications* stay active. Expired certifications must be renewed. Expired certifications are not to be considered in the workforce ~~reports~~ *metrics*.

C2.3.8. To support IA professionals, the DoD IA Portal at Defense Knowledge Online and the ~~IASE Support Environment~~ provides DoD IA policy, training requirements, and DoD-sponsored training. The DoD IA Portal is located at <http://www.us.army.mil> and the IASE is located at <http://iase.disa.mil/>.

C2.3.9. Contractor personnel supporting IA functions in Chapters 3, 4, 10, and 11 shall ~~be appropriately certified~~ *obtain the appropriate DoD-approved IA baseline certification* prior to being engaged. *Contractors have up to 6 months to obtain the rest of the qualifications for their position outlined in AP3.T1.* The contracting officer will ensure that contractor personnel are appropriately certified ~~and provide verification to the Defense Manpower Data Center (DMDC) database: <https://www.dmdc.osd.mil/dmdecomm/owa/dmde.main>~~. Additional training on local or system procedures may be provided by the DoD organization receiving services.

C2.3.10. Organizations employing LNs should coordinate in advance with appropriate offices such as the Status of Forces Agreement, the Local or Country Human Resources section of OPM, local unions, and/or training. Effective coordination will greatly enhance the capability to achieve the requirements of this Manual.

C2.3.11. Personnel IA certification status and renewal rates are management review items according to Reference (b).

C2.3.12. All personnel holding an *approved IA baseline* certification ~~listed in Appendix 3~~ in fulfillment of the requirements of this Manual must release their certification information to the Department of Defense through the Defense Workforce Certification Application (DWCA): <https://www.dmdc.osd.mil/appj/dwc/index.jsp>.



### C3. CHAPTER 3

#### IA WORKFORCE TECHNICAL CATEGORY

##### C3.1. INTRODUCTION

C3.1.1. This chapter provides detailed position guidelines and IA functions for each level within the Technical category.

C3.1.2. The functions associated with each of these levels are intended to be baseline DoD requirements. The DoD Components are expected to have additional requirements reflecting their operating policy and information system technical environment. The requirements of this Manual do not exempt individuals from meeting their own organization's standards and requirements.

##### C3.2. TECHNICAL CATEGORY DESCRIPTION

C3.2.1. This category comprises IAT Levels I, II, and III.

C3.2.2. Personnel required to perform any technical category IA functions (one or more functions) at any level must be certified to the highest level function(s) performed. An IAT position's functions for a particular level establish the basis for the individual's certification requirement.

C3.2.2.1. The IAT category's functions are cumulative. Thus, an IAT Level II or III position requires mastery of the functions of the preceding levels.

C3.2.3. IAT Category Training Requirements:

C3.2.3.1. Participation in initial training (classroom, distributive, or blended) before, or immediately on, assignment of IA responsibilities. Training need not result in award of a military specialty code (e.g., Military Occupational Specialty, Navy Enlisted Classification Code, and/or Air Force Specialty Code), but must be sufficient to meet minimum certification standards outlined here and in Appendices 2 and 3.

C3.2.3.2. Completion of an on the job skills practical evaluation to meet functional requirements listed in this chapter.

C3.2.3.3. Completion of sustainment training/continuing education as required to maintain certification status. For planning purposes the standard is normally a minimum of 20 to 40 hours annually, or 120 hours over 3 years.

C3.2.4. IAT Category Certification Requirements:

C3.2.4.1. The certification program for IAT category positions must include the functions identified for that level. All IAT category personnel, whether they perform IA functions as primary or additional/embedded duty, must be certified based on the IA functions of the position.

C3.2.4.1.1. Within 6 months of assignment of IA duties, all *military and Government civilian* IAT personnel must achieve the appropriate IA certification unless a waiver is granted per paragraphs C3.2.4.2 or C3.2.4.3.

C3.2.4.1.1.1. DoD employees and contractors performing IA functions on the effective date of this Manual have up to 4 years to comply with the certification requirements, based on DoD Component plans to meet the implementation milestones established in Chapter 9.

C3.2.4.1.1.2. New hires' qualification periods begin the date they start in the position (i.e., they must obtain the appropriate certification within 6 months of being assigned IA functions).

C3.2.4.1.2. IAT Level I certification is the minimum requirement prior to IA Managers authorizing unsupervised privileged access for personnel performing IAT Levels I through III functions described in this Chapter.

C3.2.4.2. Designated Accrediting Authorities (DAAs) may waive the certification requirement under severe operational or personnel constraints. The waiver will be documented by the DAA using a memorandum for the record stating the reason for the waiver and the plan to rectify the constraint. Waivers will not extend beyond 6 months, must include an expiration date, and be documented in the individual's IA training record. Consecutive waivers for personnel are not authorized except as noted in paragraph C3.2.4.3. Waivers must be a management review item per Reference (b). Uncertified IAT Level Is are not authorized to have unsupervised privileged access.

C3.2.4.3. IAT category personnel must be fully trained and certified prior to deployment to a combat environment. The DAA may approve a waiver for certified IAT-I's to fill level IAT-II or IAT-III billets without attaining the appropriate certification while deployed to a combat environment. The DAA may grant an interim waiver limited to the period of the deployment. The interim waiver places an individual in a suspense status and must be time limited and include an expiration date not to exceed 6 months following date of return from combat status.

C3.2.4.4. Personnel in technical category positions must be issued and retain an appointing letter to their IA duties including a statement of responsibilities for the system. Appendix 4 provides a sample statement of acceptance of responsibilities. DoD Components will appropriately edit this form and maintain a completed copy in the individual's personnel record or with the contracting officer's technical representative for contractors.

C3.2.4.5. Personnel in technical category positions must maintain certifications, as required by the certifying provider, to retain privileged system access. Level 1 certification is required prior to being authorized unsupervised privileged access.

C3.2.4.6. Personnel who are not appropriately ~~certified~~ *qualified* within 6 months of assignment to a position or who fail to maintain their certification status shall not be permitted privileged access. The DoD Components will develop programs to address remedial training and conditions for individuals to attain or return to certified status.

C3.2.4.7. The DoD Components must document and maintain the certification status of their IAT category personnel as long as they are assigned to those duties. Identification and tracking requirements are addressed in Chapter 7.

C3.2.4.8. To support the GIG infrastructure security requirements, certification standards apply equally to DoD civilian, military, and contractor personnel including those staffed by LNs (with conditional privileged access per Reference (b)).

C3.2.4.8.1. New contract language must specify certification requirements. Existing contracts must be modified, at an appropriate time during the phased implementation, to specify certification requirements.

C3.2.4.8.2. Per References (b) and (gi) and DoD 5200.2-R (Reference (hj)), LNs and Foreign Nationals (FNs) must comply with background investigation requirements and cannot be assigned to IAT Level III positions.

C3.2.4.8.3. In addition to the ~~baseline~~ IA *baseline* certification requirement for their level, IATs with privileged access must obtain appropriate Computing Environment (CE) certifications for the operating system(s) and/or security related tools/devices they support as required by their employing organization. If supporting multiple tools and devices, an IAT should obtain CE certifications for all the tools and devices they are supporting. At a minimum the IAT should obtain a certification for the tool or device he or she spends the most time supporting. For example, if an IAT is spending most of his or her time supporting security functions on a CISCO router, the IAT should obtain a CE certification for that equipment. This requirement ensures they can effectively apply IA requirements to their hardware and software systems.

C3.2.4.8.4. New hire civilian personnel must agree as a “condition of employment” that they will obtain the appropriate certification for the position to be filled.

C3.2.4.8.5. All personnel must agree to release their *IA baseline* certification qualification(s) to the Department of Defense through the DWCA.

C3.2.4.9. Technical category training requirements are summarized in Table C3.T1.

Table C3.T1. IA Technical Workforce Requirements

Civilian, Military, Contractor* (Including Civilian or Contractor LNs)	IAT Level I - III (FN and LN Levels I & II only)
Initial Training **	Yes
IA <i>Baseline</i> Certification (from approved list)	Yes (within 6 months)
Initial <del>On the Job Practical</del> <i>OJT</i> Evaluation	Yes (for initial position)
CE/ <del>OS Certification</del> <i>Certificate</i>	Yes
Maintain Certification Status	Yes (as required by certification)
Continuous Education or Sustainment Training	Yes (as required by certification (e.g., International Information Systems Security Certification Consortium, (ISC)2 requires 120 hours within 3 years for the CISSP))
Background Investigation	As required by IA level and Reference (b)
Sign Privileged Access Statement	Yes
*Contractor category, level, and certification requirements to be specified in the contract	
**Classroom, distributive, blended, government, or commercial provider	

C3.3. IAT LEVEL I

C3.3.1. IAT Level I personnel make the CE less vulnerable by correcting flaws and implementing IAT controls in the hardware or software installed within their operational systems. IAT Level I position requirements are listed in Table C3.T2.

Table C3.T2. IAT Level I Position Requirements

IAT Level I	
Attribute	Level
Experience	Normally has 0 to 5 or more years of experience in IA technology or a related field.
System Environment	CE.
Knowledge	Applies basic knowledge of IA concepts, practices, and procedures within the CE.
Supervision	Works under supervision and typically reports to a CE manager.
Other	Actions are usually authorized and controlled by policies and established procedures.
IA <i>Baseline</i> Certification & <i>CE/OS</i> <i>Certificate</i>	Within 6 months of assignment to position and mandatory for unsupervised privileged access.

C3.3.2. Table C3.T3. lists the specific functions associated with the IAT Level I position. Personnel performing these functions, regardless of their occupational title (e.g., system administrator, help desk technician, information system technician, mechanic, infantry, logistics, aviation mechanic, etc.) shall be identified as part of the IA workforce and must comply with the requirements in the tables above and C3.T1.

Table C3.T3. IAT Level I Functions

T-I.1. Recognize a potential security violation, take appropriate action to report the incident as required by regulation, and mitigate any adverse impact.
T-I.2. Apply instructions and pre-established guidelines to perform IA tasks within CE.
T-I.3. Provide end user IA support for all CE operating systems, peripherals, and applications.
T-I.4. Support, monitor, test, and troubleshoot hardware and software IA problems pertaining to their CE.
T-I.5. Apply CE specific IA program requirements to identify areas of weakness.
T-I.6. Apply appropriate CE access controls.

T-I.7.	Install and operate the IT systems in a test configuration manner that does not alter the program code or compromise security safeguards.
T-I.8.	Conduct tests of IA safeguards in accordance with established test plans and procedures.
T-I.9.	Implement and monitor IA safeguards for CE system(s) in accordance with implementation plans and standard operating procedures.
T-I.10.	Apply established IA security procedures and safeguards and comply with responsibilities of assignment.
T-I.11.	Comply with system termination procedures and incident reporting requirements related to potential CE security incidents or actual breaches.
T-I.12.	Implement online warnings to inform users of access rules for CE systems.
T-I.13.	Implement applicable patches including IA vulnerability alerts (IAVA), IA vulnerability bulletins (IAVB), and technical advisories (TA) for the CE operating system(s).
T-I.14.	Install, test, maintain, and upgrade CE operating systems software and hardware to comply with IA requirements.
T-I.15.	Understand and implement technical vulnerability corrections.
T-I.16.	Enter assets in a vulnerability management system.
T-I.17.	Apply system security laws and regulations relevant to the CE being supported.
T-I.18.	Implement DoD and DoD Component password policy.
T-I.19.	Implement specific IA security countermeasures.

### C3.4. IAT LEVEL II

C3.4.1. IAT Level II personnel provide network environment (NE) and advanced level CE support. They pay special attention to intrusion detection, finding and fixing unprotected vulnerabilities, and ensuring that remote access points are well secured. These positions focus on threats and vulnerabilities and improve the security of systems. IAT Level II personnel have mastery of the functions of the IAT Level I position. IAT Level II position requirements are listed in Table C3.T4.

Table C3.T4. IAT Level II Position Requirements

IAT Level II	
Attribute	Level
Experience	Normally has at least 3 years in IA technology or a related area.
System Environment	NE and advanced CE.
Knowledge	<ul style="list-style-type: none"> <li>• Mastery of the functions of the IAT Level I position.</li> <li>• Applies knowledge and experience with standard IA concepts, practices, and procedures within the NE.</li> </ul>
Supervision	Works under general supervision and typically reports to network manager.
Other	Relies on experience and judgment to plan and accomplish goals within the NE.
IA <i>Baseline</i> Certification & <i>CE/OS Certificate</i>	Within 6 months of assignment to position.

C3.4.2. Table C3.T5. lists the specific functions associated with the IAT Level II position. Personnel performing these functions, regardless of their occupational title (e.g., system administrator, help desk technician, information system technician, mechanic, infantry, logistics coordinator) shall be identified as part of the IA workforce and must comply with the requirements in the table above and C3.T1.

Table C3.T5. IAT Level II Functions

T-II.1.	Demonstrate expertise in IAT Level I CE knowledge and skills.
T-II.2.	Examine potential security violations to determine if the NE policy has been breached, assess the impact, and preserve evidence.
T-II.3.	Support, monitor, test, and troubleshoot hardware and software IA problems pertaining to the NE.

T-II.4.	Recommend and schedule IA related repairs in the NE.
T-II.5.	Perform IA related customer support functions including installation, configuration, troubleshooting, customer assistance, and/or training, in response to customer requirements for the NE.
T-II.6.	Provide end user support for all IA related applications for the NE.
T-II.7.	Analyze patterns of non-compliance and take appropriate administrative or programmatic actions to minimize security risks and insider threats.
T-II.8.	Manage accounts, network rights, and access to NE systems and equipment.
T-II.9.	Analyze system performance for potential security problems.
T-II.10.	Assess the performance of IA security controls within the NE.
T-II.11.	Identify IA vulnerabilities resulting from a departure from the implementation plan or that were not apparent during testing.
T-II.12.	Provide leadership and direction to IA operations personnel.
T-II.13.	Configure, optimize, and test network servers, hubs, routers, and switches to ensure they comply with security policy, procedures, and technical requirements.
T-II.14.	Install, test, maintain, and upgrade network operating systems software and hardware to comply with IA requirements.
T-II.15.	Evaluate potential IA security risks and take appropriate corrective and recovery action.
T-II.16.	Ensure that hardware, software, data, and facility resources are archived, sanitized, or disposed of in a manner consistent with system security plans and requirements.
T-II.17.	Diagnose and resolve IA problems in response to reported incidents.
T-II.18.	Research, evaluate, and provide feedback on problematic IA trends and patterns in customer support requirements.
T-II.19.	Ensure IAT Level I personnel are properly trained and have met OJT program requirements.
T-II.20.	Perform system audits to assess security related factors within the NE.
T-II.21.	Develop and implement access control lists on routers, firewalls, and other network devices.
T-II.22.	Install perimeter defense systems including intrusion detection systems, firewalls, grid sensors, etc., and enhance rule sets to block sources of malicious traffic.
T-II.23.	Work with other privileged users to jointly solve IA problems.
T-II.24.	Write and maintain scripts for the NE.
T-II.25.	Demonstrate proficiency in applying security requirements to an operating system for the NE or CE used in their current position.
T-II.26.	Implement applicable patches including IAVAs, IAVBs, and TAs for their NE.
T-II.27.	Adhere to IS security laws and regulations to support functional operations for the NE.
T-II.28.	Implement response actions in reaction to security incidents.



T-II.29. Support the design and execution of exercise scenarios.
T-II.30. Support Security Test and Evaluations (Part of C&A Process).
T-II.31. Obtain and maintain IA certification appropriate to position.

### C3.5. IAT LEVEL III

C3.5.1. IAT Level III personnel focus on the enclave environment and support, monitor, test, and troubleshoot hardware and software IA problems pertaining to the CE, NE, and enclave environments. IAT Level III personnel have mastery of the functions of both the IAT Level I and Level II positions. IAT Level III position requirements are listed in Table C3.T6.

Table C3.T6. IAT Level III Position Requirements

IAT Level III	
Attribute	Level
Experience	Normally has at least seven years experience in IA technology or a related area.
System Environment	Enclave Environment, advanced NE, and advanced CE.
Knowledge	<ul style="list-style-type: none"> <li>• Expert in all functions of both IAT Level I and IAT Level II positions.</li> <li>• Applies extensive knowledge of a variety of the IA field's concepts, practices, and procedures to ensure the secure integration and operation of all enclave systems.</li> </ul>
Supervision	<ul style="list-style-type: none"> <li>• Works independently to solve problems quickly and completely.</li> <li>• May lead and direct the work of others.</li> <li>• Typically reports to an enclave manager.</li> </ul>
Other	<ul style="list-style-type: none"> <li>• Relies on extensive experience and judgment to plan and accomplish goals for the enclave environment.</li> <li>• Supports, monitors, tests, and troubleshoots hardware and software IA problems pertaining to the enclave environment.</li> <li>• Must be a U.S. Citizen.</li> </ul>
IA <i>Baseline</i> Certification & <i>CE/OS Certificate</i>	Within 6 months of assignment to position.

C3.5.2. Table C3.T7. lists the specific functions associated with the IAT Level III position. Personnel performing these functions, regardless of their occupational title (e.g., system administrator, help desk technician, information system technician, aviation mechanic, infantry, logistics coordinator) shall be identified as part of the IA workforce and must comply with the requirements in the table above and C3.T1.

Table C3.T7. IAT Level III Functions

T-III.1. Mastery of IAT Level I and IAT Level II CE/NE knowledge and skills.
T-III.2. Recommend,-schedule, and/or implement IA related repairs within the enclave environment.
T-III.3. Coordinate and/or provide support for all enclave applications and operations.
T-III.4. Lead teams and/or support actions to quickly resolve or mitigate IA problems for the enclave environment.
T-III.5. Formulate or provide input to the enclave's IA/IT budget.
T-III.6. Support the installation of new or modified hardware, operating systems, and software applications ensuring integration with IA security requirements for the enclave.
T-III.7. Identify and/or determine whether a security incident is indicative of a violation of law that requires specific legal action.
T-III.8. Direct and/or implement operational structures and processes to ensure an effective enclave IA security program including boundary defense, incident detection and response, and key management.
T-III.9. Provide direction and/or support to system developers regarding correction of security problems identified during testing.
T-III.10. Evaluate functional operation and performance in light of test results and make recommendations regarding C&A.
T-III.11. Examine enclave vulnerabilities and determine actions to mitigate them.
T-III.12. Monitor and evaluate the effectiveness of enclave IA security procedures and safeguards.
T-III.13. Analyze IA security incidents and patterns to determine remedial actions to correct vulnerabilities.
T-III.14. Support development and/or implementation of the enclave termination plan to ensure that IA security incidents are avoided during shutdown and long term protection of archived resources is achieved.
T-III.15. Implement vulnerability countermeasures for the enclave.
T-III.16. Provide support for IA customer service performance requirements.
T-III.17. Provide support for the development of IA related customer support policies, procedures, and standards.
T-III.18. Write and maintain scripts required to ensure security of the enclave environment.

T-III.19. Implement and maintain perimeter defense systems including, but not limited to, intrusion detection systems, firewalls, grid sensors.
T-III.20. Schedule and perform regular and special backups on all enclave systems.
T-III.21. Establish enclave logging procedures to include: important enclave events; services and proxies; log archiving facility.
T-III.22. Provide OJT for IAT Level I and II DoD personnel.
T-III.23. Analyze IAVAs and Information Assurance Vulnerability Bulletins for enclave impact and take or recommend appropriate action.
T-III.24. Obtain and maintain IA certification appropriate to position.

C4. CHAPTER 4IA WORKFORCE MANAGEMENT CATEGORYC4.1. INTRODUCTION

C4.1.1. This chapter provides detailed position guidelines and IA functions for each level within the Information Assurance Management (IAM) category.

C4.1.2. The functions associated with each of these levels are intended to be baseline DoD requirements. The DoD Components are expected to have additional requirements reflecting their operating policy and information system technical environment. The requirements of this Manual do not exempt individuals from meeting their own organization's standards and requirements.

C4.2. MANAGEMENT CATEGORY DESCRIPTION

C4.2.1. This Category comprises IAM Levels I, II, and III, as well as the DAA function covered in Chapter 5. Positions required to perform IA Manager responsibilities, as established in Reference (b), and performing functions defined in this chapter are included in the Information Assurance Management category.

C4.2.2. The levels and functions in the management category are not necessarily cumulative. Table C4.T1. provides IAM category requirements.

Table C4.T1. IAM Workforce Requirements

Civilian, Military, or Contractor* (Including LNs )	IAM Level I - III (FN/LN Levels I & II** only)
Initial Training ***	Yes
IA <i>Baseline</i> Certification (from approved list)	Yes (within six months)
<i>Initial</i> OJT Evaluation	No
CE/ <i>OS</i> Certificate	No
Maintain Certification Status	Yes (as required by certification)
<i>Continuous Education or</i> Sustainment Training	Yes (as required by certification (e.g., (ISC)2 requires 120 hours within 3 years for CISSP))
Background Investigation	As required by IA level and Reference (b)

\*Requirements to be stated in contract  
 \*\* FN/LN IAM Level II must meet conditions of References (b), (*gi*) and (*hj*)  
 \*\*\*Classroom, distributive, blended, *government*, or commercial provider

### C4.2.3. IAM Category Certification Requirements:

C4.2.3.1. The certification requirement for IAM category positions includes all the functions identified for that level. All management category personnel, whether they perform IA functions as primary or as an additional/embedded duty, will be certified based on the IA functions of the position.

C4.2.3.1.1. Personnel required to perform any management category IA function(s) (one or more functions) at any level must be certified to the highest level function(s) performed. An IAM position's functional requirement(s) for a particular level establish the basis for the certification requirement.

C4.2.3.1.2. IAM positions that also perform IAT functions must also obtain the appropriate technical level certification and complete the other IAT level requirements prior to being granted unsupervised privileged access.

C4.2.3.2. Within 6 months of assignment of IA duties, management category *military and Government civilian* personnel must achieve the appropriate IA *baseline* certification for their level. The requirements in paragraphs C3.2.4.1.1.1. and C3.2.4.1.1.2. for current and new hire DoD employees also apply to IAMs.

C4.2.3.2.1. DAAs may waive the certification requirement under severe operational or personnel constraints. The waiver will be documented by the DAA using a memorandum for the record stating the reason for the waiver and the plan to rectify the constraint.

C4.2.3.2.2. Waivers will not extend beyond 6 months and must include an expiration date and be documented in the individual IA training record. Consecutive waivers for personnel are not authorized except as noted in paragraph C4.2.3.4.2. Waivers must be a management review item.

C4.2.3.3. Personnel in management category positions must maintain certifications, as required by their *ir* certification provider, ~~as described in Appendix 3,~~ to retain their *ir* position.

C4.2.3.4. Personnel not certified within 6 months of assignment of IA duties or who fail to maintain their certified status will not be permitted to carry out the responsibilities of the position. The DoD Components must develop programs to address remedial training and to establish conditions allowing management personnel to return to certified status.

C4.2.3.4.1. If after appropriate remediation efforts individuals do not meet certification requirements, they must be reassigned to other duties.

C4.2.3.4.2. IAM category personnel must be fully trained and certified prior to deployment to a combat environment. However, the DAA may grant an interim waiver for

personnel required to fill IAM II or III level billets with IAM I or IAM II certified individuals who cannot obtain the appropriate certification while deployed in a combat environment. The interim waiver may be granted by the DAA for the period of deployment. The interim waiver places an individual in a suspense status and must be time limited and include an expiration date not to exceed 6 months following the date of return from the combat environment.

C4.2.3.5. The DoD Components must document and maintain the certification status of their management category personnel as long as they are assigned to those duties. Identification and tracking requirements are addressed in Chapter 7.

C4.2.3.6. Personnel in management category positions will retain an appointing letter assigning them IA responsibilities for their system(s) per Reference (b). If a management category position requires IA privileged access, a statement of responsibility for the system(s) will also be executed per Reference (b). Appendix 4 provides a sample statement of acceptance of responsibilities.

C4.2.3.7. In support of GIG infrastructure security requirements, certification standards apply equally to DoD civilian, military, contractor personnel, and LNs.

C4.2.3.7.1. New contract language must specify certification requirements. Existing contracts must be modified to specify certification requirements during the phased implementation described in Chapter 9.

C4.2.3.7.2. LNs or FNs may be conditionally assigned to IAM Level II but may not be assigned to IAM Level III positions (per Reference (b)). They must comply with background investigation requirements per Reference (h).

### C4.3. IAM LEVEL I

C4.3.1. IAM Level I personnel are responsible for the implementation and operation of a DoD IS or system DoD Component within their CE. Incumbents ensure that IA related IS are functional and secure within the CE. IAM Level I position requirements are listed in Table C4.T2.

Table C4.T2. IAM Level I Position Requirements

IAM Level I	
Attribute	Level
Experience	Usually an entry level management position with 0 to 5 or more years of management experience.
System Environment	CE IAM.
Knowledge	Applies knowledge of IA policy, procedures, and structure to develop, implement, and maintain a secure CE.
Supervision	<ul style="list-style-type: none"> <li>For IA issues, typically reports to an IAM Level II (NE).</li> </ul>

	<ul style="list-style-type: none"> <li>• May report to other management for other CE operational requirements.</li> </ul>
Other	Manages IA operations for a CE system(s).
IA <i>Baseline</i> Certification	Within 6 months of assignment to position.

C4.3.2. Table C4.T3. lists the specific functions associated with the IAM Level I position. Personnel performing these functions, regardless of their occupational title (e.g., ISSO, IAO, ISSM, logistics manager, pilot, infantry officer) shall be identified as part of the IA workforce and must comply with the requirements in the table above and C4.T1.

Table C4.T3. IAM Level I Functions

M-I.1. Use federal and organization specific published documents to manage operations of their CE system(s).
M-I.2. Provide system related input on IA security requirements to be included in statements of work and other appropriate procurement documents.
M-I.3. Support and administer data retention and recovery within the CE.
M-I.4. Participate in the development or modification of the computer environment IA security program plans and requirements.
M-I.5. Validate users' designation for IT Level I or II sensitive positions, per Reference (b).
M-I.6. Develop procedures to ensure system users are aware of their IA responsibilities before granting access to DoD information systems.
M-I.7. Recognize a possible security violation and take appropriate action to report the incident, as required.
M-I.8. Supervise or manage protective or corrective measures when an IA incident or vulnerability is discovered.
M-I.9. Ensure that system security configuration guidelines are followed.
M-I.10. Ensure that IA requirements are integrated into the Continuity of Operations Plan (COOP) for that system or DoD Component.
M-I.11. Ensure that IA security requirements are appropriately identified in computer environment operation procedures.
M-I.12. Monitor system performance and review for compliance with IA security and privacy requirements within the computer environment.

M-I.13. Ensure that IA inspections, tests, and reviews are coordinated for the CE.
M-I.14. Participate in an IS risk assessment during the Certification and Accreditation process.
M-I.15. Collect and maintain data needed to meet system IA reporting requirements.
M-I.16. Obtain and maintain IA <i>baseline</i> certification appropriate to position.

#### C4.4. IAM LEVEL II

C4.4.1. IAM Level II personnel are responsible for the IA program of an IS within the NE. Incumbents in these positions perform a variety of security related tasks, including the development and implementation of system information security standards and procedures. They ensure that IS are functional and secure within the NE. IAM Level II position requirements are listed in Table C4.T4.

Table C4.T4. IAM Level II Position Requirements

IAM Level II	
Attribute	Level
Experience	Usually has at least five years of management experience.
System Environment	NE IAM.
Knowledge	Applies knowledge of IA policy, procedures, and workforce structure to develop, implement, and maintain a secure NE.
Supervision	<ul style="list-style-type: none"> <li>• For IA issues, typically reports to an IAM Level III (Enclave) Manager or DAA.</li> <li>• May report to other senior management for network operational requirements.</li> </ul>
Other	<ul style="list-style-type: none"> <li>• Relies on experience and judgment to plan and accomplish goals.</li> <li>• Manages IA operations for a NE(s).</li> </ul>
IA <i>Baseline</i> Certification	Within six months of assignment to position.

C4.4.2. Table C4.T5. lists the specific functions associated with the IAM Level II position. Personnel performing these functions, regardless of their occupational title (e.g., ISSO, IAO, ISSM, logistics manager, pilot, infantry officer) shall be identified as part of the IA workforce and must comply with the requirements in the table above and C4.T1.



Table C4.T5. IAM Level II Functions

M-II.1.	Develop, implement, and enforce policies and procedures reflecting the legislative intent of applicable laws and regulations for the NE.
M-II.2.	Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the security of network system(s) operations.
M-II.3.	Develop NE security requirements specific to an IT acquisition for inclusion in procurement documents.
M-II.4.	Recommend resource allocations required to securely operate and maintain an organization's NE IA requirements.
M-II.5.	Participate in an IS risk assessment during the C&A process.
M-II.6.	Develop security requirements for hardware, software, and services acquisitions specific to NE IA security programs.
M-II.7.	Ensure that IA and IA enabled software, hardware, and firmware comply with appropriate NE security configuration guidelines, policies, and procedures.
M-II.8.	Assist in the gathering and preservation of evidence used in the prosecution of computer crimes.
M-II.9.	Ensure that NE IS recovery processes are monitored and that IA features and procedures are properly restored.
M-II.10.	Review IA security plans for the NE.
M-II.11.	Ensure that all IAM review items are tracked and reported.
M-II.12.	Identify alternative functional IA security strategies to address organizational NE security concerns.
M-II.13.	Ensure that IA inspections, tests, and reviews are coordinated for the NE.
M-II.14.	Review the selected security safeguards to determine that security concerns identified in the approved plan have been fully addressed.
M-II.15.	Evaluate the presence and adequacy of security measures proposed or provided in response to requirements contained in acquisition documents.
M-II.16.	Monitor contract performance and periodically review deliverables for conformance with contract requirements related to NE IA, security, and privacy.
M-II.17.	Provide leadership and direction to NE personnel by ensuring that IA security awareness, basics, literacy, and training are provided to operations personnel commensurate with their responsibilities.
M-II.18.	Develop and implement programs to ensure that systems, network, and data users are aware of, understand, and follow NE and IA policies and procedures.
M-II.19.	Advise the DAA of any changes affecting the NE IA posture.

M-II.20. Conduct an NE physical security assessment and correct physical security weaknesses.
M-II.21. Help prepare IA certification and accreditation documentation.
M-II.22. Ensure that compliance monitoring occurs, and review results of such monitoring across the NE.
M-II.23. Obtain and maintain IA <i>baseline</i> certification appropriate to position.

#### C4.5. IAM LEVEL III

C4.5.1. IAM Level III personnel are responsible for ensuring that all enclave IS are functional and secure. They determine the enclaves' long term IA systems needs and acquisition requirements to accomplish operational objectives. They also develop and implement information security standards and procedures through the DoD certification and accreditation process. IAM Level III position requirements are listed in Table C4.T6.

Table C4.T6. IAM Level III Position Requirements

IAM Level III	
Attribute	Level
Experience	Usually has at least 10 years of management experience.
System Environment	Enclave Environment IAM.
Knowledge	Applies knowledge of IA policy, procedures, and workforce structure to develop, implement, and maintain a secure enclave environment.
Supervision	<ul style="list-style-type: none"> <li>• Typically reports to a DAA for IA issues.</li> <li>• May report to other senior managers for enclave operational requirements.</li> </ul>
Other	<ul style="list-style-type: none"> <li>• Must be a U.S. Citizen.</li> <li>• Relies on extensive experience and judgment to plan and accomplish enclave security related goals.</li> <li>• Manages IA operations for an enclave(s).</li> </ul>
IA <i>Baseline</i> Certification	Within 6 months of assignment to position.

C4.5.2. Table C4.T7. lists the specific functions associated with the IAM Level III position. Personnel performing these functions, regardless of their occupational title (e.g., ISSO, IAO, ISSM, logistics manager, pilot, infantry officer) shall be identified as part of the IA workforce and must comply with the requirements in the table above and C4.T1.

Table C4.T7. IAM Level III Functions

M-III.1.	Securely integrate and apply Department/Agency missions, organization, function, policies, and procedures within the enclave.
M-III.2.	Ensure that protection and detection capabilities are acquired or developed using the IS security engineering approach and are consistent with DoD Component level IA architecture.
M-III.3.	Ensure IAT Levels I – III, IAM Levels I and II, and anyone with privileged access performing IA functions receive the necessary initial and sustaining IA training and certification(s) to carry out their IA duties.
M-III.4.	Prepare or oversee the preparation of IA certification and accreditation documentation.
M-III.5.	Participate in an IS risk assessment during the C&A process.
M-III.6.	Ensure information ownership responsibilities are established for each DoD IS and implement a role based access scheme.
M-III.7.	Analyze, develop, approve, and issue enclave IA policies.
M-III.8.	Evaluate proposals to determine if proposed security solutions effectively address enclave requirements, as detailed in solicitation documents.
M-III.9.	Identify IT security program implications of new technologies or technology upgrades.
M-III.10.	Evaluate cost benefit, economic and risk analysis in decision making process.
M-III.11.	Interpret and/or approve security requirements relative to the capabilities of new information technologies.
M-III.12.	Interpret patterns of non compliance to determine their impact on levels of risk and/or overall effectiveness of the enclave's IA program.
M-III.13.	Analyze identified security strategies and select the best approach or practice for the enclave.
M-III.14.	Ensure that security related provisions of the system acquisition documents meet all identified security needs.
M-III.15.	Evaluate and approve development efforts to ensure that baseline security safeguards are appropriately installed.
M-III.16.	Evaluate the presence and adequacy of security measures proposed or provided in response to requirements contained in acquisition documents.

M-III.17.	Take action as needed to ensure that accepted products meet Common Criteria requirements as stated in Reference (b).
M-III.18.	Monitor and evaluate the effectiveness of the enclaves' IA security procedures and safeguards to ensure they provide the intended level of protection.
M-III.19.	Provide enclave IA guidance for development of the COOP.
M-III.20.	Ensure all IAM review items are tracked and reported.
M-III.21.	Advise the DAA of changes affecting the enclave's IA posture.
M-III.22.	Obtain and maintain IA <i>baseline</i> certification appropriate to position.

## C5. CHAPTER 5

### DESIGNATED ACCREDITING AUTHORITY (DAA) REQUIREMENTS

#### C5.1. INTRODUCTION

C5.1.1. Reference (~~h~~) directs that a DAA be appointed for each DoD information system operating within, or on behalf of, the Department of Defense. It requires that all DAAs be U.S. citizens. They must also be DoD employees, with a level of authority allowing them to accept, in writing, the risk of operating DoD ISs under their purview. Reference (a) further requires that all DoD personnel be adequately trained and certified in order to perform the tasks associated with their IA responsibilities and makes the heads of the DoD Components responsible for ensuring that DAAs are appointed for all DoD Component ISs.

C5.1.1.1. DAA functions may be performed on a full- or part-time basis by a DoD civilian or military employee in the designated role.

C5.1.1.2. DAA performing other management functions such as IAM-II or IAM-III, must also meet the training and certification requirements for those categories and levels.

C5.1.2. All personnel performing DAA functions must satisfy both preparatory and sustaining DoD training and certification requirements.

#### C5.2. DAA FUNCTIONS AND RESPONSIBILITIES

##### C5.2.1. DAA Functional Description

C5.2.1.1. The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk.

C5.2.1.2. Establishes and directs the long term goals, policies, and procedures relating to the IS security requirements.

C5.2.1.3. Ensures that the policies, systems, and procedures comply with and support IA requirements.

C5.2.1.4. Given a final report requesting approval to operate an IS at a specified level of trust, the DAA will analyze and judge the information for validity and reliability to ensure the system is able to operate at the proposed level of security.

C5.2.1.5. Review accreditation documents to confirm the level of risk is acceptable for an IS. This decision will be made by weighing the system mission requirements against the identified level of risk per DoD Instruction 8510.01 (Reference (~~ik~~)) (or its successor documents)

and implemented countermeasures to known vulnerabilities. Additional factors to consider include system architecture, system security measures, system operations policy, system security management plan, and provisions for system operator and end-user training.

C5.2.1.6. Table C5.T1. lists the DAA's functions.

Table C5.T1. DAA Functions

DAA.1.	Grant the authority to operate an IS or network at an acceptable level of risk.
DAA.2.	Review accreditation documents to confirm that the level of risk is within acceptable limits for each network and/or IS.
DAA.3.	Verify that each IS complies with IA requirements.
DAA.4.	Ensure establishment, administration, and coordination of security for systems that Component personnel or contractors operate.
DAA.5.	Ensure the program manager defines the system security requirements for acquisitions.
DAA.6.	Manages the IA workforce. Assigns IA responsibilities to the individuals reporting directly to the DAA.
DAA.7.	Ensures individuals filling IA positions are assigned in writing, trained, certified, and sign a statement of responsibilities.
DAA.8.	Assign the mission assurance category in accordance with References (b) and (f) for each IS and approve the classification level required for the applications implemented on them.
DAA.9.	Allocate resources to achieve and maintain an acceptable level of security and to remedy security deficiencies.
DAA.10.	Resolve issues regarding those systems requiring multiple or joint accreditation. This may require documentation of condition or agreements in Memoranda of Agreement.
DAA.11.	Ensure that, when classified or sensitive unclassified information is exchanged between ISs or networks (internal or external), the content of this communication is protected from unauthorized observation or modification by acceptable means.

### C5.3. DAA TRAINING AND CERTIFICATION REQUIREMENT

C5.3.1. Each assigned DAA must:

C5.3.1.1. Complete the DoD DAA computer-based training (CBT) or Web-based training (WBT) product within 60 days of assignment to the position. The CBT, titled "DAA, Designated Accrediting Authority," is located on the DoD IA Portal for those with a CAC or directly from IASE.

C5.3.1.2. The DAA and the unit training officer will sign the DAA CBT certificate upon completion of the DISA DAA Certification Course (Figure C5.F1.).

C5.3.1.3. Maintain the course completion certificate (Figure C5.F1.), also available at the DoD IA Portal, as a part of the DAA's official personnel file.

C5.3.1.4. Recertify every 3 years.

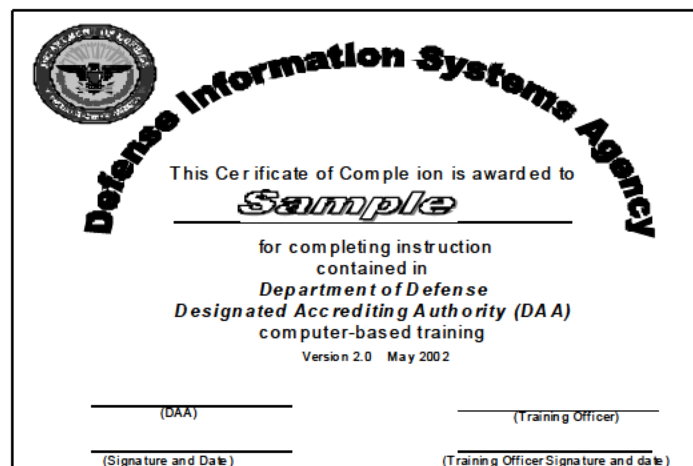
C5.3.2. The DAA may substitute the following National Defense University/Information Resource Management College Courses for the DoD DAA CBT:

C5.3.2.1. Computer Network Security Systems Instruction No. 4012 (DAA) course and certificate. The IRMC official transcript shall be used to document completion of the requirement.

C5.3.2.2. The Information System Certification and Accreditation course (catalog # 6209). The IRMC Transcript will serve as proof of Completion.

C5.3.3. The DoD Components are encouraged to provide additional training specific to their unique requirements.

Figure C5.F1. Sample DAA Certificate of Completion



## C6. CHAPTER 6

### AUTHORIZED USER MINIMUM IA AWARENESS REQUIREMENTS

#### C6.1. INTRODUCTION

C6.1.1. IT has enabled the Department of Defense to transmit, communicate, collect, process, and store unprecedented amounts of information.

C6.1.2. Increasing dependence on information systems has focused attention on the need to ensure that these assets, and the information they process, are protected from actions that would jeopardize the DoD's ability to effectively function.

C6.1.3. Responsibility for securing the Department's information and systems lies with the DoD Components. The trained and aware user is the first and most vital line of defense.

C6.1.4. IT users need to maintain a degree of understanding about IA policies and doctrine commensurate with their responsibilities. They must be capable of appropriately reporting and responding to suspicious activities, and know how to protect the information and IT systems to which they have access.

C6.1.5. IA training must be current, engaging, and relevant to the target audience to enhance its effectiveness. Its primary purpose is to educate and influence behavior. The focus must be on education and awareness of threats and vulnerabilities so users do not perform actions that lead to or enable exploitations of the DoD ISSs. Authorized users must understand that they are a critical link in their organization's overall IA success.

C6.1.6. DISA's DoD IA Awareness CBT is the DoD baseline standard. It meets all DoD level requirements for end user awareness training. DISA will ensure it provides distributive awareness content to address evolving requirements promulgated by Congress, the OMB under the ISS LoB for Tier I, or the Office of the Secretary of Defense. DISA's training products can be accessed via the DoD IA Portal for those with a CAC or directly from IASE.

C6.1.7. The DoD Components are required to use the DoD SSC as their IA Awareness Provider. The DoD IA Awareness Course will be used to meet the initial and annual training mandated by this Manual and Reference (c). However, Components are expected to address organization specific topics and local incident reporting procedures.

C6.1.8 The DoD SSC Intelligence Community IA Awareness Training product meets all DoD requirements and may be substituted for the DoD SSC IA Awareness Training product.

#### C6.2. GENERAL REQUIREMENTS



C6.2.1 The requirements for computer security awareness training have been established under the authority of 2224 of title 10, United States Code; section 278g-3 of title 15, United States Code; and OMB Circular A-130 (References (j*l*), (~~k~~*m*), and (~~l~~*n*)). References (b) and (~~g~~*i*) implement the requirements and extend it to IA.

C6.2.2. To ensure understanding of the critical importance of IA, all individuals with access to DoD IT systems are required to receive and complete initial IA awareness training before being granted access to the system(s) and annual IA awareness training to retain access.

C6.2.3. The DoD Components must document and maintain the status of awareness compliance for each user. Required versus actual IA awareness will be a management review item.

C6.2.4. All users will be informed of their information and IS security responsibilities, and consent to monitoring.

C6.2.5. At a minimum, the following themes must be conveyed in IA initial annual awareness programs:

C6.2.5.1. Critical reliance on information and IS resources.

C6.2.5.2. Commitment to protect information and IS resources to include personal identifiable information.

C6.2.5.3. Threats, vulnerabilities, and related risks associated with IS.

C6.2.5.4. Consequences for inadequate protection of the organization's IS resources.

C6.2.5.5. The essential role of the DoD employee.

### C6.3. SPECIFIC REQUIREMENTS

User awareness programs shall address the topics specified in ISS LoB, Reference (~~m~~*o*), to include but not limited to the following:

C6.3.1. The importance of IA to the organization and to the authorized user.

C6.3.2. Relevant laws, policies, and procedures, and how they affect the authorized user (e.g., copyright, ethics, and standards of conduct).

C6.3.3. Examples of external threats such as script kiddies, crackers, hackers, protesters, or agents in the employ of terrorist groups or foreign countries.

C6.3.4. Examples of internal threats such as malicious or incompetent authorized users, users in the employ of terrorist groups or foreign countries, disgruntled employees or Service members, hackers, crackers, and self-inflicted intentional or unintentional damage.

C6.3.5. The potential elevated sensitivity level of aggregated unclassified information.

C6.3.6. Authorized user risk from social engineering.

C6.3.7. Common methods to protect critical system information and procedures.

C6.3.8. Principles of shared risk in networked systems (i.e., how a risk assumed by one person is imposed on the entire network) and changes in the physical environment (e.g., water, fire, and dust/dirt).

C6.3.9. Risks associated with remote access (e.g., telecommuting, during deployment, or on temporary duty).

C6.3.10. Legal requirements regarding privacy issues, such as email status (see DoD Directive 1000.25 (Reference ~~np~~)) and the need to protect systems containing payroll, medical and personnel records.

C6.3.11. Knowledge of malicious code (e.g., logic bomb, Trojan horse, malicious mobile code, viruses, and worms) including how they attack, how they damage an IS, how they may be introduced inadvertently or intentionally, and how users can mitigate their impact.

C6.3.12. The impact of distributed denial of service attacks and what users can do to mitigate them.

C6.3.13. How to prevent self-inflicted damage to system information security through disciplined application of IA procedures such as proper logon, use of passwords, preventing spillage of classified information, e-mail security, etc.

C6.3.14. Embedded software and hardware vulnerabilities, how the Department of Defense corrects them (e.g., IAVA process), and the impact on the authorized user.

C6.3.15. Prohibited or unauthorized activity on DoD systems (e.g., peer-to-peer file sharing, gambling, personal use, and gain issues).

C6.3.16. Requirements and procedures for reporting spillage, unauthorized or suspicious activity, and local IA office point of contact information.

C6.3.17. Categories of information classification and differences between handling information on the Non-Classified Internet Protocol Router Network (NIPRNet) or the SECRET Internet Protocol Router Network (SIPRNet).

C6.3.18. Software issues including license restrictions on DoD systems, encryption, and media sanitation requirements and procedures.

C6.3.19. Requirements and procedures for transferring data to/from a non-DoD network.

C6.3.20. Requirements and procedures for protection of Data at Rest.

C6.3.21. Requirements and procedures for sharing information.

## C7. CHAPTER 7

### IA WORKFORCE IDENTIFICATION, TRACKING, AND ASSIGNMENT

#### C7.1. INTRODUCTION

C7.1.1. The Department of Defense must manage its IA workforce effectively and efficiently to provide trained, skilled personnel who will protect the operation of its IS.

C7.1.2. The DoD Components will leverage existing manpower and personnel databases, learning management systems, other tools, and procedures to support effective management of their IA workforces.

C7.1.3. Tools and procedures must enable the assignment and tracking of qualified personnel both within the DoD Components and in support of joint assignments.

C7.1.4. As a prerequisite to effective IA management, the DoD Components must identify all positions and personnel with IA responsibilities, regardless of occupational specialty, or whether the duty is performed as primary or as an additional/embedded duty. Positions and personnel will be aligned to an IA category, specialty and level, per Chapters 3, 4, 5, 10, and 11, and documented in the appropriate database(s). IA Workforce data elements must comply with requirements established in Reference (b), and DoD Instruction 7730.64, DoD Instruction 1336.5, and DoD Instruction 7730.54 (References (eq), (pr), and (qs)).

C7.1.5. The DoD Components must use, to the extent possible, existing personnel/manpower and unit organizational databases, such as DCPDS, to satisfy the requirements outlined in this chapter. DoD Components are responsible for providing this information per References (pr) and (qs) for military members. DoD Instruction 1444.2 (Reference (ft)) dictates DoD civilian database requirements.

C7.1.6. The Defense Manpower Data Center (DMDC) will leverage DoD Component provided information on civilian and military IA positions and personnel to support development of an integrated picture of the DoD IA workforce per Chapter 8 and References (b), (eq), (pr), (qs), and (ft).

#### C7.2. IA WORKFORCE MANAGEMENT

C7.2.1. The DoD Components must identify military, civilian, and contractor personnel performing IA functions whether performed as their primary duty, or as an additional/embedded duty. Chapters 3, 4, 5, 10, and 11 provide a DoD standard naming convention and descriptions of IA categories, specialties, levels, and their related functions.

C7.2.2. Identify all positions required to perform IA functions, by category or specialty and level, in manpower tables of organization. Identification of the IA workforce positions must be a management review item.

C7.2.3. Assign appropriately trained and certified personnel to IA positions (internal and joint positions), per Chapters 2-5, 10 and 11.

C7.2.4. Require each individual assigned IA responsibilities to sign a statement of responsibilities appropriate for that position. Appendix 4 provides a recommended statement of responsibilities for privileged access users.

C7.2.5. Track IA personnel training and certification against position requirements. Positions required to perform functions in more than one category or level of management, technical, or specialized IA functions must be identified individually in the appropriate manpower database. Personnel filling these positions must be aligned with the position and maintain the appropriate certification/qualifications for each.

C7.2.6. ~~Report~~ *Collect metrics* on DoD Component training (including awareness) and certification programs in accordance with Chapter 8.

### C7.3. IA WORKFORCE IDENTIFICATION REQUIREMENTS

C7.3.1. To manage the IA workforce effectively, the DoD Components must comply with the following requirements for each employee group.

#### C7.3.2. Civilians:

C7.3.2.1. DoD personnel in the 2210 job series and other civilian IA job series (e.g., 0854, 1550) General Schedule (GS) ~~or occupation code (NSPS)~~ shall be classified by GS ~~or NSPS~~ parenthetical specialty title. They must indicate a primary title based on the position's primary or paramount duties. They must also indicate a secondary parenthetical specialty title if performing additional/embedded duties beyond those primary duties.

C7.3.2.2. Identify all civilian positions and personnel required to perform IA functions described in this Manual in the appropriate database(s) (e.g., DCPDS, e-Joint Manpower and Personnel System (e-JMAPS), or equivalent), including Local Nationals, performing IA functions, regardless of series, and align them with the categories and levels described in Chapters 3, 4, 5, 10, and 11. IA workforce management ~~reporting metrics~~ includes the following:

C7.3.2.2.1. All IA positions, regardless of whether IA functions are performed as a primary duty, or as an additional/embedded duty.

C7.3.2.2.2. Certification status of incumbent including certification or recertification date, cost of certification/recertification test, and associated training (if paid by the government).

C7.3.2.2.3. Waivers granted for personnel filling IA positions.

C7.3.2.3. Verify that DCPDS or its equivalent has the correct data (down to the parenthetical specialty level for the series).

C7.3.2.4. Use the DCPDS Special civilian titling to align ~~reporting~~ *workforce metrics* across the Department of Defense based on the following:

C7.3.2.4.1. Use the existing authorized Position Specialty Code, “INFOSEC,” to support IA workforce identification and management requirements across the Department of Defense. The DoD Components will ensure that DCPDS reflects the following guidance:

C7.3.2.4.2. All positions in the 2210 or other civilian IA job series (e.g., 0854, 1550) must comply with Office of Personnel Management (OPM) guidance on standardized titling. Positions in job series with primary or additional/embedded IA functions must enter at least one but not more than two authorized parenthetical titles.

C7.3.2.4.3. Ensure that all DoD civilian positions and personnel with IA functions, regardless of OPM series or job title, use “INFOSEC” as the Position Specialty Code (PSC) in the Defense Civilian Personnel Data System. The PSC allows identification of a DoD civilian position with IA functions regardless of OPM series or job title. The abbreviation for Security, “INFOSEC,” established in this Manual, supports civilian IA workforce identification and management requirements across the Department of Defense.

C7.3.3. Military:

C7.3.3.1. Identify all military positions and personnel required to perform IA functions described in this Manual in the appropriate database(s) (e.g., e-JMAPS, or DoD Component Manpower/Personnel Systems), including Foreign Nationals, regardless of occupational specialty, and align them with the categories and levels described in Chapters 3-5, 10, and 11.

C7.3.3.2. Identify the following, regardless of occupational specialty, in, e-JMAPS, or the DoD Component manpower and/or personnel management systems, as appropriate:

C7.3.3.2.1. All IA positions, regardless of whether IA responsibilities are performed as a primary duty, or as an additional/embedded duty.

C7.3.3.2.2. All personnel performing IA functions.

C7.3.3.2.3. Certification status of incumbent including certification or recertification date, cost of certification/recertification test, and associated training (if paid by the government).

C7.3.3.3. Assign a code to each IA position that identifies its category or specialty and level, and the corresponding minimum certification requirements per Chapters 3-5, 10, 11, and Appendix 3.

C7.3.3.4. Assign a code to individuals based on their certification level.

C7.3.3.5. Match the certified individuals against required positions.

C7.3.3.6. Track the IA workforce against the required positions.

C7.3.4. Contractors

C7.3.4.1. Identify all contractors performing IA functions and align them with the categories and levels described in Chapters 3, 4, 10, and 11.

C7.3.4.2. Ensure that contractor personnel, including LNs, have the appropriate IA certification and background investigation.

C7.3.4.3. Ensure the capability to ~~report~~ *collect metrics* in detail on individual contractor employee certification(s) and certification status.

C7.3.4.4. Specify contractor certification and training requirements in all contracts that include acquisition of IA services. Eligible contractor personnel must have their IA certification and function level documented in DMDC supported application which will support tracking contractors IA category or specialty, level, and certification qualification.

C7.3.4.5. Contracting officers' technical representatives will enter the required data into the DMDC application which will support tracking contractors IA category, specialty, level, and certification qualification.

## C8. CHAPTER 8

### IA WORKFORCE MANAGEMENT REPORTING AND METRICS

#### C8.1. INTRODUCTION

C8.1.1. To manage its IA workforce effectively and efficiently, and provide trained and ~~certified~~ *qualified* personnel when and where needed, the Department of Defense must know IA position requirements, the existing IA workforce and its qualifications, and where these critical assets are employed.

C8.1.2. The ~~reporting requirements and workforce~~ metrics outlined in this chapter support the DoD current and long term management of critical IA personnel resources.

C8.1.3. The DoD Components must use, to the extent possible, existing personnel/manpower/unit organizational databases and tools to satisfy these IA reporting *and workforce management metrics* requirements.

C8.1.4. The IA WIP Annual Report is due at the end of the ~~Calendar Year~~ *fiscal year* and will ~~leverage support~~ the Federal Information Security Management Act (FISMA) report (Reference (c)) ~~workforce data~~ requirements. The IA WIP Annual Report consolidates IA ~~training, certification, qualification~~ and workforce management reporting requirements per References (a), (b), (~~fh~~), (~~gi~~), and (~~hj~~).

#### C8.2. REPORTING *AND IA WORKFORCE METRICS* REQUIREMENTS

C8.2.1. ASD(NII)/DoD CIO coordinates IA Training and Certification Program ~~reporting management~~ requirements, and ensures that collected information supports ASD(NII)/DoD CIO validation of DoD IA workforce readiness. Each DoD Component must provide DMDC with the individual and position level data required to populate the tables in Figure C8.F1., which will be used to generate the IA WIP Annual Report *to support FISMA requirements and IA workforce management at each level of the DoD*.

C8.2.2. All the DoD Components are required to submit data on the status of their IA workforce for inclusion in the IA WIP Annual Report.

C8.2.3. The DoD Components will provide both qualitative and quantitative information. The information reported will support the following IA workforce management critical information requirements:

C8.2.3.1. Methodologies used to identify employees required to perform IA functions.

C8.2.3.2. Training and certification requirements developed by the DoD Components for employees performing IA functions.



C8.2.3.3. Tracking processes used to determine requirements for how many employees perform IA functions and have received IA training and certification.

C8.2.3.4. Plans and methodologies to track, monitor, and document completion of IA awareness training for all network users.

C8.2.3.5. The ASD(NII)/DoD CIO will review and validate/approve the methodologies and processes reported by the DoD Components to implement and maintain the DoD baseline requirements of this Manual.

C8.2.4. To support DoD IA Workforce management requirements, the ASD(NII)/DoD CIO will combine *metrics* from the DoD Components to assemble a consolidated IA WIP Annual Report *and status*. The IA WIP Annual Report will include DoD Component comments regarding IA workforce lessons learned, issues from the previous calendar year, and plans for the next. It will also provide statistics for personnel performing IA functions on a primary or additional/embedded duty basis, broken down by IA category, specialty and level.

C8.2.5. In addition to the reporting requirements outlined in this chapter, ASD(NII)/DoD CIO will gather data on numerous aspects of the IA workforce including recruitment, retention, training, and impact on IA operations. This data will be combined with the DoD Component submitted reports to develop a comprehensive picture of the IA workforce and its operational effectiveness.

~~C8.2.6. The DoD Components will submit qualitative data as part of IA WIP annual reporting that describes the methodologies, requirements, and processes used to implement the requirements of Reference (a) and this Manual. Specifically, the DoD Components will report:~~

~~C8.2.6.1. Methodologies used to identify employees in the IA workforce.~~

~~C8.2.6.2. Training and certification requirements developed for employees in the IA workforce such as:~~

~~C8.2.6.2.1. DoD Component schools/training centers IA related curriculum status and actual/planned annual throughput. Highlight accomplishments and initiatives and describe any partnerships/cooperative arrangements with other DoD entities and/or the private sector (i.e., industry and academia) regarding IA curriculum program activities.~~

~~C8.2.6.2.2. DoD Component specific training and certification requirements including the operating system requirement in addition to the DoD baseline requirements.~~

~~C8.2.6.2.3. Programs to train and certify personnel performing IA functions. Highlight key features (e.g., needs self assessment) and accomplishments to include number and percent of total participants completing training and certification.~~

~~C8.2.6.3. Tracking processes used to determine how many employees are in the IA workforce, are properly certified, and have received the required training.~~

~~C8.2.6.4. Status of recruitment and retention for the IA workforce, indicating if it is increasing, stable, or decreasing, and why.~~

~~C8.2.6.5. Plans and methodologies used to track, monitor, and document completion of IA awareness training for all network users.~~

~~C8.2.6.6. Programs for IA awareness in the workforce. Highlight key features of the program and major accomplishments.~~

~~C8.2.6.7. Provide evidence to substantiate/explain reported completion rates for the IA awareness program requirement.~~

~~C8.2.6.8. IA curriculum/treatment in CAPSTONE, officer accession programs, Flag, Commanding Officer/Executive Officer, and Warrant Officer indoctrination and Component professional military education courses, as applicable including resident, distributive, and blended.~~

~~C8.2.6.9. Defense/Service colleges, universities, and professional military education. IA related curriculum, its status, and actual/planned annual throughput, including resident, distributive, and/or blended. Highlight any IA related accomplishments and initiatives; including partnerships/cooperative arrangements with other DoD entities, and/or the private sector (e.g., industry or academia).~~

C8.2.76. The DoD Components will submit quantitative data as part of IA WIP annual reporting that identifies its positions, number filled, and qualifications of the personnel filling them to support both DoD FISMA reporting and the DoD CIO's IA workforce management responsibility.

C8.2.76.1. Each DoD Component must ensure that its personnel and staffing databases are properly configured, per References (θq) through (ϕt), to capture the following quantitative data. If a given metric cannot be captured to a database it must be collected manually and included with the submission of the qualitative data described above.

C8.2.76.2. IA workforce positions and manning status. ~~(This is a management review item.)~~

C8.2.76.2.1. Number of IA positions by category, specialty and level.

C8.2.76.2.1.1. Primary duty IA positions.

C8.2.76.2.1.2. Additional/embedded duty IA positions.

C8.2.76.2.2. Number of IA positions filled, by category or specialty, and level.

C8.2.~~76~~.2.3. Number of IA positions filled with ~~certified~~ *qualified* incumbents by category or specialty and level.

C8.2.~~76~~.3. Personnel ~~certified~~ *qualified* levels: (This is a management review item.)

C8.2.~~76~~.3.1. Number of personnel ~~certified~~ *qualified*, by category or specialty, and level.

C8.2.~~76~~.3.2. Number of personnel ~~certified~~ *qualified*, by category, specialty, and level who are actually filling an IA position.

~~C8.2.73.3.3. Number of personnel who were recertified during the current year.~~

~~C8.2.73.3.4. Number of waivers granted for personnel filling IA positions.~~

~~C8.2.7.4. Total dollars obligated or expended for IA training and certification (including courses leading to certification).~~

~~C8.2.7.5. Compliance with the workforce certification continuing education and sustainment training requirement.~~

C8.2.~~76~~.64. Number of users who completed the IA awareness training requirement versus total number of authorized users. (This is a management review item.)

C8.2.~~87~~. The IA WIP Annual Report covers 1 ~~January~~ *October* through ~~4 December~~ *30 September* each ~~calendar~~ *fiscal* year. Each DoD Component must provide the DMDC with individual and position level data required to populate the tables in Figure C8.F1 for the preceding ~~Calendar~~ *fiscal* year. The DoD Components will submit their qualitative information to ASD NII/DoD CIO by ~~31 January~~ *30 September* for the preceding ~~calendar~~ *fiscal* year. The DMDC will create a consolidated report capturing the DoD Components' IA Workforce ~~Data~~ *Metrics* reflected in the tables in Figure C8.F1. (Note: LNs are included in two employee groups: Civilian and Contractor. LN includes all individuals working for the Department of Defense in a foreign country who are nationals or non U.S. residents of that country).

C8.2.~~98~~. The IA WIP Annual Report *referred to in paragraphs C1.4.1.5., C8.1.4., C8.2.1., C8.2.2., C8.2.4., C8.2.6., C8.2.7., and Figure C8.F1. of this issuance* has been assigned report control symbol DD-NII(A)2274 in accordance with *the procedures in* DoD 8910.1-M (Reference (~~su~~)).

*Preparation of this report/study cost the Department of Defense a total of approximately \$188,000 in Fiscal Years 2012 - 2017.*  
*Generated on 2011Nov15 1034*

*RefID: 5-2B2C687*

Figure C8.F1. IA WIP Annual Report Format *Workforce Metrics*

Table 1: IA Workforce Primary Duty Positions

	Civilian			Military			Contractor	
	Number	Filled	Certified Qualified* / Waiver	Number	Filled	Certified Qualified* / Waiver	Filled	Certified Qualified* / Waiver
IAT I								
IAT II								
IAT III								
IAM I								
IAM II								
IAM III								
CND-A								
CND- IS								
CND-IR								
CND-AU								
CND-SPM								
IASAE I								
IASAE II								
IASAE III								
Total								

\**Certified Qualified* in accordance with the policy for that position. *Report* waivers ~~must be~~ approved by the DAA (see paragraph C3.2.4.2., C3.2.4.3., C4.2.3.2., or C4.2.3.4.2.) *separately from qualified (e.g., 100/10)*. Count personnel filling IAT, CND-SP, IASAE, and IAM Category or specialty positions in all categories or specialties according to C2.2.5. and AP2.1.2.3.

Table 2: IA Workforce Additional/Embedded Duty Positions

	Civilian			Military			Contractor	
	Number	Filled	Certified Qualified* / Waiver	Number	Filled	Certified Qualified* / Waiver	Filled	Certified Qualified* / Waiver
IAT I								
IAT II								
IAT III								
IAM I								
IAM II								
IAM III								
CND-A								
CND- IS								
CND-IR								
CND-AU								
CND-SPM								
IASAE I								
IASAE II								
IASAE III								
Total								

\*~~Certified~~ *Qualified* in accordance with the policy for that position. *Report* waivers ~~must be~~ approved by the DAA (see paragraph C3.2.4.2., C3.2.4.3., C4.2.3.2., or C4.2.3.4.2.) *separately from qualified* (e.g., 100/10). Count personnel filling IAT, CND-SP, IASAE, IAM Category or Specialty positions in all categories per C2.2.5. and AP2.1.2.3.

**Table 3: IA Workforce Certification/Recertification**

-	Civilian		Military		Contractor	
-	Required	Recertified	Required	Recertified	Required	Recertified
IAT-I	-	-	-	-	-	-
IAT-II	-	-	-	-	-	-
IAT-III	-	-	-	-	-	-
IAM-I	-	-	-	-	-	-
IAM-II	-	-	-	-	-	-
IAM-III	-	-	-	-	-	-
CND-A						
CND-IS						
CND-IR						
CND-AU						
CND-SPM						
IASAE-I						
IASAE-II						
IASAE-III						
<b>Total</b>	-	-	-	-	-	-

## C9. CHAPTER 9

### IA WORKFORCE IMPLEMENTATION REQUIREMENTS

#### C9.1. INTRODUCTION

C9.1.1. This chapter provides guidance to support a coordinated and orderly transition from the legacy systems and processes to full compliance with the DoD's requirements. These actions require in-depth budget and personnel management planning.

C9.1.2. Adhering to the categories, specialties and levels outlined is critical to support the effective identification of the IA workforce across the Department of Defense. Standardizing skill sets supports joint assignments and system interoperability.

#### C9.2. GENERAL REQUIREMENTS

C9.2.1. The DoD Components must:

C9.2.1.1. Plan for, and incrementally complete, these requirements over four years from the effective date of this manual. Complete requirements to this Manual within 5 years from the publication date (1 extra year to implement CND-SP and IASAE Specialties).

C9.2.1.2. Develop and submit to the IA WIPAC implementation policies, processes, and plans to support compliance with the requirements outlined below within 6 months of the publication date of this Manual.

C9.2.1.3. Provide representation to the IA WIPAC as required in Chapter 1.

~~C9.2.1.4. Report progress annually, against implementation requirements, to ASD(NII)/DoD CIO, using the format presented in Figure C9.F1.~~

#### C9.3. SPECIFIC REQUIREMENTS

C9.3.1. To allow for proper identification and planning of requirements, the Department of Defense has adopted a phased approach to this implementation. The first year provides time for the identification of specific requirements to support budget and staffing planning, and to certify the initial 10 percent of the IA workforce. The next 3 years provide time to bring the full IA workforce into compliance with the requirements in phases. Thirty percent of the workforce must come into compliance each year, as outlined below.

C9.3.2. Within 12 months of the effective date of this Manual, the DoD Components must:

C9.3.2.1. Provide Component IA Manager and Human Resource Management participation in the DoD sponsored Component Implementation Workshop that will be conducted by the Defense-wide Information Assurance Program (DIAP) Office within three months of publication of this Manual.

C9.3.2.2. Identify all positions per Chapters 3-5, 7, 10 and 11, required to execute the IA functions listed in Chapters 3-5, 10 and 11 as primary or additional/embedded duties.

C9.3.2.3. Assign IA workforce category, specialty and level codes for the Component's staffing and personnel data systems based on the categories and levels described in Chapters 3-5, 10 and 11. These codes must be identified to DMDC per References (~~eq~~), (~~pr~~), (~~qs~~), and (~~rt~~). The data elements will be routinely captured by the DMDC and formatted to support the DoD's IA workforce management requirements. If a Component uses a personnel or manpower system or database that does not exchange data with DMDC systems, develop the necessary data fields to track IA workforce requirements.

C9.3.2.4. Budget for IA training, certification, and workforce management requirements of DoD government personnel, as described below. The budget plan must ensure implementation of the requirements over a three year period, and must specifically include resources for:

C9.3.2.4.1. Staffing identified IA positions (primary or additional/embedded duty).

C9.3.2.4.2. Training incumbents.

C9.3.2.4.3. Ensuring staffing and unit databases/tools are upgraded to support IA workforce management requirements as appropriate.

C9.3.2.4.4. Training for staffing managers on the systems and processes required to support the IA workforce training and management requirements.

C9.3.2.4.5. Certifying (including training and testing) current and planned IA workforce members.

C9.3.2.5. The DoD Components must plan to meet the following milestones. The milestone plan will begin with the next planning, program, and budget cycle to execute these requirements beginning in Calendar Year (CY)-07. The phases of this implementation approach are:

C9.3.2.5.1. Year One (CY-07): Identify IA workforce positions, fill 10 percent of the IA positions with certified personnel. Develop budget to support follow-on implementation years two–four.

C9.3.2.5.2. Year Two (CY-08): Fill a total of 40 percent of the IA positions with certified personnel.

C9.3.2.5.3. Year Three (CY-09): Fill a total of 70 percent of the IA positions with certified personnel.

C9.3.2.5.4. Year Four (CY-10): All IAT and IAM Category positions are held by certified personnel.

C9.3.2.5.5. Year Five (CY-11): All CND-SP and IASAE Specialty positions are held by certified personnel.

C9.3.2.5.6. Thereafter, all incumbents and new hires must be trained, certified, and recertified in accordance with this Manual.

#### ~~C9.4. IMPLEMENTATION PLAN REPORTING REQUIREMENTS~~

~~C9.4.1. The DoD Components must report progress to ASD(NII)/DoD CIO on budgeting to meet implementation requirements using the format in Figure C9.F1. The Information Assurance Workforce Milestone Budget Plan Report is exempt from licensing in accordance with the provisions of paragraph C4.4.6. of Reference (su).~~

~~C9.4.2. The IA Workforce Implementation Milestone Budget Plan report is due 31 July each year for five years from the date of publication of this Manual.~~

~~Figure C9.F1. IA Workforce Milestone Budget Plan Report~~

<del>IA Workforce Milestone Budget Plans (training and certification, costs)</del>								
<del>IA-WF Budget</del>	<del>PY</del>	<del>CY</del>	<del>BY00</del>	<del>BY01</del>	<del>BY02</del>	<del>BY03</del>	<del>BY04</del>	<del>Total</del>
<del>Required</del>		-	-	-	-	-	-	-
<del>Budgeted</del>								
<del>Obligated</del>		-	-	-	-	-	-	-

~~PY = Previous Year, CY = Current Year, BY = Budget Year~~



C10. CHAPTER 10IA WORKFORCE SYSTEM ARCHITECT AND ENGINEER (IASAE) SPECIALTYC10.1. INTRODUCTION

C10.1.1. This chapter provides detailed position guidelines and IA functions for each level within the IASAE specialty.

C10.1.2. The functions associated with each of these levels are intended to be baseline DoD requirements. The DoD Components are expected to have additional requirements reflecting their operating policy and information system technical environment. The requirements of this Manual do not exempt individuals from meeting their own organization's standards and requirements.

C10.2. IASAE SPECIALTY DESCRIPTION

C10.2.1. This specialty comprises IASAE Levels I, II, and III.

C10.2.2. The levels and functions in the IASAE specialty are not necessarily cumulative. Table C10.T1. summarizes IASAE position requirements.

Table C10.T1. IASAE Workforce Requirements

Civilian, Military or Contractor* (Including LNs )	IASAE Level I – III (FN/LN Levels I and II** only)
Initial Training ***	Yes
IA <i>Baseline</i> Certification (from approved list)	Yes (within 6 months)
<i>Initial</i> OJT Evaluation	No
<i>CE/OS Certification Certificate</i>	No
Maintain Certification Status	Yes (as required by certification)
<i>Continuous Education or Sustainment Training</i>	Yes (as required by certification (e.g., (ISC)2 requires 120 hours within 3 years for the CISSP))
Background Investigation	As required by IA level and Reference (b)
*Requirements to be stated in contract	
**FN/LN IASAE Level II must meet conditions of References (b), ( <del>g</del> i) and ( <del>h</del> j)	
***Classroom, distributive, blended, <i>government</i> , or commercial provider	

### C10.2.3. IASAE Specialty Certification Requirements:

C10.2.3.1. The certification requirement for IASAE specialty positions includes all the functions identified for that level. All IASAE specialty personnel, whether they perform IA functions as primary or as an additional/embedded duty, will be certified based on the IA functions of the position.

C10.2.3.1.1. Personnel required to perform any IASAE specialty IA function(s) (one or more functions) at any level must be certified to the highest level function(s) performed. An IASAE position's functional requirement(s) for a particular level establish the basis for the certification requirement.

C10.2.3.1.2. IASAE positions that also perform IAT functions must also obtain the appropriate computing environment certification and complete the other IAT level requirements prior to being granted unsupervised privileged access.

C10.2.3.2. Within 6 months of assignment of IA duties, IASAE specialty *military and Government civilian* personnel must achieve the appropriate IA *baseline* certification for their level.

C10.2.3.2.1. New hires' qualification periods begin the date they start in the position (i.e., they must obtain the appropriate certification within 6 months of being assigned IA functions).

C10.2.3.2.2. DoD employees and contractors performing IA functions on the effective date of this Manual have up to 4 years to comply with the certification requirements, based on DoD Component plans to meet the implementation milestones established in Chapter 9.

C10.2.3.2.3. DAAs may waive the certification requirement under severe operational or personnel constraints. The waiver will be documented by the DAA using a memorandum for the record stating the reason for the waiver and the plan to rectify the constraint.

C10.2.3.2.4. Waivers will not extend beyond 6 months, must include an expiration date, and be documented in the individual's IA training record. Consecutive waivers for personnel are not authorized except as noted in paragraph C10.2.3.4.2. Waivers must be a management review item.

C10.2.3.3. Personnel in IASAE specialty positions must maintain certifications, as required by their *ir* certification provider, ~~as described in Appendix 3,~~ to retain their *ir* position.

C10.2.3.4. Personnel not certified within 6 months of assignment of IA duties or who fail to maintain their certified status will not be permitted to carry out the responsibilities of the position. The DoD Components must develop programs to address remedial training and to establish conditions allowing IASAE personnel to return to certified status.

C10.2.3.4.1. Individuals continuing to not meet certification requirements after appropriate remediation efforts shall be reassigned to other duties.

C10.2.3.4.2. IASAE specialty personnel must be fully trained and certified prior to deployment to a combat environment. However, the DAA may grant an interim waiver for the period of the deployment for IASAE personnel to fill IASAE billets one level higher than their current certification. The interim waiver places an individual in a suspense status and must be time limited and include an expiration date not to exceed 6 months following the date of return from the combat environment.

C10.2.3.5. The DoD Components must document and maintain the certification status of their IASAE specialty personnel as long as they are assigned to those duties. Identification and tracking requirements are addressed in Chapter 7.

C10.2.3.6. Personnel in IASAE specialty positions will retain an appointing letter assigning them IA responsibilities for their system(s) in accordance with Reference (b). If an IASAE specialty position requires IA privileged access, a statement of responsibility for the system(s) will also be executed in accordance with Reference (b). Appendix 4 provides a sample statement of acceptance of responsibilities.

C10.2.3.7. In support of GIG infrastructure security requirements, certification standards apply equally to DoD civilian, military, contractor personnel, and LNs.

C10.2.3.7.1. New contract language must specify certification requirements. Existing contracts must be modified to specify certification requirements during the phased implementation described in Chapter 9.

C10.2.3.7.2. LNs or FNs may be conditionally assigned to IASAE Level II but may not be assigned to IASAE Level III positions in compliance with Reference (b). IASAE positions/personnel with privileged access or management functions must comply with background investigation requirements in Table E3.T1. of Reference (b).

### C10.3. IASAE LEVEL I

C10.3.1. IASAE Level I personnel are responsible for the design, development, implementation, and/or integration of a DoD IA architecture, system, or system component for use within their CE. Incumbents ensure that IA related IS will be functional and secure within the CE. IASAE Level I position requirements are listed in Table C10.T2.

Table C10.T2. IASAE Level I Position Requirements

IASAE Level I	
Attribute	Level
Experience	Usually an entry level IASAE position with 0 or more years of IASAE experience.

System Environment	CE IASAE.
Knowledge	Applies knowledge of IA policy, procedures, and structure to design, develop, and implement CE system(s), system components, or system architectures.
Supervision	<ul style="list-style-type: none"> <li>• For IA issues, typically reports to an IASAE Level II, IAM, or DAA.</li> <li>• May report to other management for other CE operational requirements.</li> </ul>
Other	Actions are usually authorized and controlled by policies and established procedures.
IA <i>Baseline</i> Certification	Within 6 months of assignment to position.

C10.3.2. Table C10.T3. lists the specific functions associated with the IASAE Level I position. Positions responsible for performing any of these functions, regardless of the incumbent's occupational title (Engineer, Scientist, Computer Specialist, ISSO, IAO, ISSM, manager, pilot, infantry officer, etc.) shall be identified as part of the IA workforce and must comply with the requirements in Tables C10.T1. and C10.T2.

Table C10.T3. IASAE Level I Functions

IASAE-I.1. Identify information protection needs for CE system(s) and network(s).
IASAE-I.2. Define CE security requirements in accordance with applicable IA requirements (e.g., Reference (b), Director Central Intelligence Directive 6/3 (Reference (tv)), organizational security policies).
IASAE-I.3. Provide system related input on IA security requirements to be included in statements of work and other appropriate procurement documents.
IASAE-I.4. Design security architectures for CE system(s) and network(s).
IASAE-I.5. Design and develop IA or IA-enabled products for use within a CE.
IASAE-I.6. Integrate and/or implement Cross Domain Solutions (CDS) for use within a CE.
IASAE-I.7. Design, develop, and implement security designs for new or existing CE system(s). Ensure that the design of hardware, operating systems, and software applications adequately address IA security requirements for the CE.
IASAE-I.8. Design, develop, and implement system security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation.

IASAE-I.9. Develop and implement specific IA countermeasures for the CE.
IASAE-I.10. Develop interface specifications for CE system(s).
IASAE-I.11. Develop approaches to mitigate CE vulnerabilities, recommend changes to system or system components as needed.
IASAE-I.12. Ensure that system designs support the incorporation of DoD-directed IA vulnerability solutions, e.g., IAVAs.
IASAE-I.13. Develop IA architectures and designs for DoD IS with basic integrity and availability requirements, to include MAC III systems as defined in References (b) and ( <del>f</del> h); systems with a Basic Level-of-Concern for availability or integrity in accordance with Reference ( <del>t</del> w); and other DAA designated systems.
IASAE-I.14. Develop IA architectures and designs for systems processing Sensitive Compartmented Information (SCI) that will operate at Protection Level 1 or 2 as defined in Reference ( <del>t</del> v).
IASAE-I.15. Assess threats to and vulnerabilities of CE system(s).
IASAE-I.16. Identify, assess, and recommend IA or IA-enabled products for use within a CE; ensure recommended products are in compliance with the DoD evaluation and validation requirements of References (b) and ( <del>f</del> h).
IASAE-I.17. Ensure that the implementation of security designs properly mitigate identified threats.
IASAE-I.18. Assess the effectiveness of information protection measures utilized by CE system(s).
IASAE-I.19. Ensure security deficiencies identified during security/certification testing have been mitigated, corrected, or a risk acceptance has been obtained by the appropriate DAA or authorized representative.
IASAE-I.20. Provide input to IA C&A process activities and related documentation (system life-cycle support plans, concept of operations, operational procedures and maintenance training materials, etc.).
IASAE-I.21. Participate in an IS risk assessment during the C&A process and design security countermeasures to mitigate identified risks.
IASAE-I.22. Provide engineering support to security/certification test and evaluation activities.

IASAE-I.23. Document system security design features and provide input to implementation plans and standard operating procedures.
IASAE-I.24. Recognize a possible security violation and take appropriate action to report the incident.
IASAE-I.25. Implement and/or integrate security measures for use in CE system(s) and ensure that system designs incorporate security configuration guidelines.
IASAE-I.26. Ensure the implementation of CE IA policies into system architectures.
IASAE-I.27. Obtain and maintain IA <i>baseline</i> certification appropriate to position.

#### C10.4. IASAE LEVEL II

C10.4.1. IASAE Level II positions are responsible for the design, development, implementation, and/or integration of a DoD IA architecture, system, or system component for use within the NE. Incumbents ensure that IA related IS will be functional and secure within the NE. IASAE Level II position requirements are listed in Table C10.T4.

Table C10.T4. IASAE Level II Position Requirements

IASAE Level II	
Attribute	Level
Experience	Usually has at least 5 years of IASAE experience.
System Environment	NE IASAE.
Knowledge	Applies knowledge of IA policy, procedures, and workforce structure to design, develop, and implement a secure NE.
Supervision	<ul style="list-style-type: none"> <li>• For IA issues, typically reports to an IASAE Level III, IAM, or DAA.</li> <li>• May report to other senior IASAE for network operational requirements.</li> </ul>
Other	<ul style="list-style-type: none"> <li>• Relies on experience and judgment to plan and accomplish goals.</li> <li>• LN opportunities are extremely limited and must meet requirements of Table E3.T1. of Reference (b).</li> </ul>
IA <i>Baseline</i> Certification	Within 6 months of assignment to position.

C10.4.2. Table C10.T5. lists the specific functions associated with the IASAE Level II position. Positions responsible for performing any of these functions, regardless of the incumbent's occupational title (Engineer, Scientist, Computer Specialist, ISSO, IAO, ISSM, manager, pilot, infantry officer, etc.) shall be identified as part of the IA workforce and must comply with the requirements in Tables C10.T4. and C10.T1.

Table C10.T5. IASAE Level II Functions

IASAE-II.1. Identify information protection needs for the NE.
IASAE-II.2. Define NE security requirements in accordance with applicable IA requirements (e.g., References (b) and (tu) and organizational security policies).
IASAE-II.3. Provide system related input on IA security requirements to be included in statements of work and other appropriate procurement documents.
IASAE-II.4. Design security architectures for use within the NE.
IASAE-II.5. Design and develop IA or IA-enabled products for use within a NE.
IASAE-II.6. Integrate and/or implement CDS for use within a CE or NE.
IASAE-II.7. Develop and implement security designs for new or existing network system(s). Ensure that the design of hardware, operating systems, and software applications adequately address IA security requirements for the NE.
IASAE-II.8. Design, develop, and implement network security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation.
IASAE-II.9. Design, develop, and implement specific IA countermeasures for the NE.
IASAE-II.10. Develop interface specifications for the NE.
IASAE-II.11. Develop approaches to mitigate NE vulnerabilities and recommend changes to network or network system components as needed.
IASAE-II.12. Ensure that network system(s) designs support the incorporation of DoD-directed IA vulnerability solutions, e.g., IAVAs.
IASAE-II.13. Develop IA architectures and designs for DoD IS with medium integrity and availability requirements, to include MAC II systems as defined in References (b) and (fh), systems with a medium Level-of-Concern for availability or integrity in accordance with Reference (tv), and other DAA designated systems.

IASAE-II.14. Develop IA architectures and designs for systems processing SCI that will operate at Protection Level 1 or 2 as defined in Reference ( <del>tv</del> ).
IASAE-II.15. Assess threats to and vulnerabilities of the NE.
IASAE-II.16. Identify, assess, and recommend IA or IA-enabled products for use within an NE; ensure recommended products are in compliance with the DoD evaluation and validation requirements of References (b) and ( <del>fh</del> ).
IASAE-II.17. Ensure that the implementation of security designs properly mitigate identified threats.
IASAE-II.18. Assess the effectiveness of information protection measures used by the NE.
IASAE-II.19. Evaluate security architectures and designs and provide input as to the adequacy of security designs and architectures proposed or provided in response to requirements contained in acquisition documents.
IASAE-II.20. Ensure security deficiencies identified during security/certification testing have been mitigated, corrected, or a risk acceptance has been obtained by the appropriate DAA or authorized representative.
IASAE-II.21. Provide input to IA C&A process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).
IASAE-II.22. Participate in an IS risk assessment during the C&A process and design security countermeasures to mitigate identified risks.
IASAE-II.23. Provide engineering support to security/certification test and evaluation activities.
IASAE-II.24. Document system security design features and provide input to implementation plans and standard operating procedures.
IASAE-II.25. Recognize a possible security violation and take appropriate action to report the incident.
IASAE-II.26. Implement and/or integrate security measures for use in network system(s) and ensure that system designs incorporate security configuration guidelines.
IASAE-II.27. Ensure the implementation of NE IA policies into system architectures.
IASAE-II.28. Ensure the implementation of subordinate CE IA policies is integrated into the NE system architecture.



IASAE-II.29. Obtain and maintain IA *baseline* certification appropriate to position.**C10.5. IASAE LEVEL III**

C10.5.1. IASAE Level III positions are responsible for the design, development, implementation, and/or integration of a DoD IA architecture, system, or system component for use within CE, NE, and enclave environments. They ensure that the architecture and design of DoD IS are functional and secure. This may include designs for program of record systems and special purpose environments with platform IT interconnectivity. Incumbents may also be responsible for system or network designs that encompass multiple CE and/or NE to include those with differing data protection/classification requirements. IASAE Level III position requirements are listed in Table C10.T6.

Table C10.T6. IASAE Level III Position Requirements

IASAE Level III	
Attribute	Level
Experience	Usually has at least 10 years of IASAE experience.
System Environment	Enclave Environment IASAE.
Knowledge	Applies knowledge of IA policy, procedures, and workforce structure to design, develop, and implement a secure enclave environment.
Supervision	<ul style="list-style-type: none"> <li>• Typically reports to a DAA for IA issues.</li> <li>• May report to other senior managers for enclave operational requirements.</li> </ul>
Other	<ul style="list-style-type: none"> <li>• Must be a U.S. Citizen.</li> <li>• Relies on extensive experience and judgment to plan and accomplish enclave security related goals.</li> <li>• May also serve in a management/oversight capacity for an enclave(s).</li> </ul>
IA <i>Baseline</i> Certification	Within 6 months of assignment to position.

C10.5.2. Table C10.T7. lists the specific functions associated with the IASAE Level III position. Positions responsible for performing any of these functions, regardless of the incumbents' occupational title (Chief Engineer, Engineer, Scientist, Computer Specialist, ISSO, IAO, ISSM, manager, pilot, infantry officer, etc) shall be identified as part of the IA workforce and must comply with the requirements in Tables C10.T6. and C10.T1.

Table C10.T7. IASAE Level III Functions

IASAE-III.1.	Identify information protection needs for the enclave environment.
IASAE-III.2.	Define enclave security requirements in accordance with applicable IA policies (e.g., References (b) and (t)) and organizational security policies).
IASAE-III.3.	Provide input on IA security requirements to be included in statements of work and other appropriate procurement documents.
IASAE-III.4.	Support Program Managers responsible for the acquisition of DoD IS to ensure IA architecture and systems engineering requirements are properly addressed throughout the acquisition life-cycle.
IASAE-III.5.	Design security architectures for use within the enclave environment.
IASAE-III.6.	Design and develop IA or IA-enabled products for use within the enclave.
IASAE-III.7.	Design and develop CDS for use within CE, NE, or enclave environments.
IASAE-III.8.	Develop and implement security designs for new or existing enclave system(s). Ensure that the design of hardware, operating systems, and software applications adequately address IA security requirements for the enclave.
IASAE-III.9.	Design, develop, and implement security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation for the enclave environment.
IASAE-III.10.	Design, develop, and implement specific IA countermeasures for the enclave.
IASAE-III.11.	Develop interface specifications for use within the enclave environment.
IASAE-III.12.	Develop approaches to mitigate enclave vulnerabilities and recommend changes to system or system components as needed.
IASAE-III.13.	Ensure that enclave system(s) and network(s) designs support the incorporation of DoD-directed IA vulnerability solutions, e.g., IAVAs.

IASAE-III.14. Develop IA architectures and designs for DoD IS with high integrity and availability requirements, to include MAC I systems as defined in References (b) and ( <del>fh</del> ), systems with a high Level-of-Concern for availability or integrity in accordance with Reference ( <del>tv</del> ), and other DAA designated systems.
IASAE-III.15. Develop IA architectures and designs for systems and networks with multilevel security requirements or requirements for the processing of multiple classification levels of data (e.g., UNCLASSIFIED, SECRET, and TOP SECRET).
IASAE-III.16. Develop IA architectures and designs for systems processing SCI that will operate at Protection Level 3, 4, or 5 as defined in Reference ( <del>tv</del> ).
IASAE-III.17. Develop IA architectures and designs for DoD IS to include automated IS applications, enclaves (which include networks), and special purpose environments with platform IT interconnectivity, e.g., weapons systems, sensors, medical technologies, or distribution systems.
IASAE-III.18. Ensure that acquired or developed system(s) and network(s) employ Information Systems Security Engineering and are consistent with DoD Component level IA architecture.
IASAE-III.19. Assess threats to and vulnerabilities of the enclave.
IASAE-III.20. Identify, assess, and recommend IA or IA-enabled products for use within an enclave and ensure recommended products are in compliance with the DoD evaluation and validation requirements of References (b) and ( <del>fh</del> ).
IASAE-III.21. Ensure that the implementation of security designs properly mitigate identified threats.
IASAE-III.22. Assess the effectiveness of information protection measures utilized by the enclave.
IASAE-III.23. Evaluate security architectures and designs and provide input as to the adequacy of security designs and architectures proposed or provided in response to requirements contained in acquisition documents.
IASAE-III.24. Ensure security deficiencies identified during security/certification testing have been mitigated, corrected, or a risk acceptance has been obtained by the appropriate DAA or authorized representative.
IASAE-III.25. Provide input to IA C&A process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).

IASAE-III.26. Participate in an IS risk assessment during the C&A process and design security countermeasures to mitigate identified risks.
IASAE-III.27. Provide engineering support to security/certification test and evaluation activities.
IASAE-III.28. Document system security design features and provide input to implementation plans and standard operating procedures.
IASAE-III.29. Recognize a possible security violation and take appropriate action to report the incident.
IASAE-III.30. Implement and/or integrate security measures for use in the enclave and ensure that enclave designs incorporate security configuration guidelines.
IASAE-III.31. Ensure the implementation of enclave IA policies into system architectures.
IASAE-III.32. Ensure the implementation of subordinate CE and NE IA policies are integrated into the enclave system architecture.
IASAE-III.33. Oversee and provide technical guidance to IASAE Level I and II personnel.
IASAE-III.34. Obtain and maintain IA <i>baseline</i> certification appropriate to position.

## C11. CHAPTER 11

### COMPUTER NETWORK DEFENSE-SERVICE PROVIDER (CND-SP) SPECIALTY

#### C11.1. INTRODUCTION

C11.1.1. This chapter provides detailed guidelines and CND-SP functions for each level within the CND-SP specialty. The requirements of this Manual apply to CND-SP established and accredited in accordance with Reference (*gi*).

C11.1.2. The functions associated with this specialty are intended to be baseline DoD requirements. Each CND-SP is expected to have additional requirements reflecting its operating policy, specific organizational mission, and technical operating environment. The requirements of this Manual do not exempt individuals from meeting their own organization's standards and requirements.

#### C11.2. CND-SP SPECIALTY DESCRIPTION

C11.2.1. This specialty is comprised of the following:

C11.2.1.1. CND-SP Analyst (CND-A)

C11.2.1.2. CND-SP Infrastructure Support (CND-IS)

C11.2.1.3. CND-SP Incident Responder (CND-IR)

C11.2.1.4. CND-SP Auditor (CND-AU)

C11.2.1.5. CND-SP Manager (CND-SPM)

C11.2.2. Personnel assigned to accredited CND-SPs will normally occupy a position corresponding to a single CND-SP specialty. In cases where personnel perform functions corresponding to multiple CND-SP specialties, their position should be designated based on the CND-SP specialty that most closely aligns to the position's primary responsibility and functions.

C11.2.3. The following are CND-SP specialty training requirements:

C11.2.3.1. Participation in initial formal training (classroom, distributive, *government*, or blended) before or immediately upon assignment of Computer Network Defense (CND) responsibilities. Training does not need to result in the award of a military category code (e.g., Military Occupational Specialty, Navy Enlisted Specialty Code, and/or Air Force Specialty Code), but must be sufficient to meet minimum certification standards outlined here and in Appendices 2 and 3.

C11.2.3.2. Completion of an on-the-job skills practical evaluation to meet functional requirements listed in this chapter (except CND-SPM).

C11.2.3.3. Completion of sustainment training/continuing education as required to maintain certification status. For planning purposes the standard is normally a minimum of 20 to 40 hours annually, or 120 hours over 3 years.

C11.2.4. The following are CND technical specialty certification requirements:

C11.2.4.1. The certification program for CND-SP specialty positions must include the functions identified for that level. All CND-SP specialty personnel must be certified based on their primary CND position.

C11.2.4.1.1. Within 6 months of assignment to an accredited CND-SP position, all CND-SP specialty *military and Government civilian* personnel must achieve the appropriate CND certification unless a waiver is granted in accordance with paragraphs C11.2.4.2. or C11.2.4.3.

C11.2.4.1.2. DoD employees or contractors performing CND functions on the effective date of this Manual have up to 4 years to comply with these requirements, based on DoD Component plans to meet the implementation milestones established in Chapter 9.

C11.2.4.1.3. The qualification period for new hires begins the date they start in the position (i.e., they must obtain the appropriate certification within 6 months of being assigned CND functions).

C11.2.4.2. USSTRATCOM may waive the certification requirement under severe operational or personnel constraints. The waiver will be documented by the USSTRATCOM using a memorandum for the record stating the reason for the waiver and the plan to rectify the constraint. Waivers will not extend beyond 6 months, must include an expiration date, and be documented in the individual's CND training record. Consecutive waivers for personnel are not authorized except as noted in paragraph C11.2.4.3. Waivers must be a management review item in accordance with Reference (b).

C11.2.4.3. CND-SP specialty personnel must be fully trained and certified prior to deployment to a combat environment. USSTRATCOM may approve a waiver for certified CND-SP billets without attaining the appropriate CND-SP specific certification while deployed to a combat environment (however, CND-SP specialty personnel must have the appropriate baseline IAT or IAM Certification). USSTRATCOM may grant an Interim Waiver limited to the period of the deployment. The interim waiver places an individual in a suspense status, which must be time limited and include an expiration date not to exceed 6 months following the date of return from combat status.

C11.2.4.4. Personnel in CND-SP specialty positions must maintain certifications, as required by the certification provider, to retain the CND-SP position.

C11.2.4.5. Personnel who are not appropriately certified within 6 months of assignment to a position or who fail to maintain their certification status shall not be permitted to execute the responsibilities of the position. The DoD Components will develop programs to address remedial training and conditions for individuals to attain or return to certified status.

C11.2.4.6. The DoD Components must document and maintain the certification status of their CND-SP specialty personnel as long as they are assigned to those duties. Identification and tracking requirements are addressed in Chapter 7.

C11.2.4.7. To support the GIG infrastructure security requirements, certification standards apply equally to DoD civilian, military, including those staffed by LNs (with conditional privileged access according to Reference (b)), and contractor personnel.

C11.2.4.7.1. New contract language must specify certification requirements. Existing contracts must be modified, at an appropriate time during the phased implementation, to specify certification requirements.

C11.2.4.7.2. In addition to the baseline CND certification requirement for their level, privileged users must obtain CE certifications as required by their employing organization to ensure they can effectively apply CND requirements to those systems.

C11.2.4.7.2.1. New hire civilian personnel must agree as a “condition of employment” that they will obtain and maintain the appropriate certification for the position.

C11.2.4.7.2.2. All personnel must agree to release their certification qualification(s) to the Department of Defense.

C11.2.4.8. CND-SP specialty training requirements are summarized in Table C11.T1.

Table C11.T1. Accredited CND-SP Workforce Requirements

Civilian, Military, Contractor* (Including Civilian or Contractor LNs)	CND-A, CND-IS, CND-IR, CND-AU, CND-SPM
Initial Training **	Yes
<del>CND IA</del> Baseline Certification (from approved list)	Yes (within 6 months)
Initial OJT Evaluation	Yes (except CND-SPM)
<del>CE/OS Certification Certificate</del>	Yes (except CND-SPM)
Maintain Certification Status	Yes (as required by certification)
Continuous Education or Sustainment Training	Yes As Required by Certification

	(e.g., (ISC)2 requires 120 hours triennially for the CISSP )
Background Investigation	As required by CND level and Reference (b)
Sign Privileged Access Statement	Yes
*Contractor specialty, level, and certification requirements to be specified in the contract	
**Classroom, Distributive, Blended, Government, or Commercial Provider	

### C11.3. CND-A

C11.3.1. CND-A personnel use data collected from a variety of CND tools (including intrusion detection system alerts, firewall and network traffic logs, and host system logs) to analyze events that occur within their environment. Individuals within CND-SPs who collect and analyze event information or perform threat or target analysis duties within the CND-SP shall be considered CND-As. CND-A position requirements are listed in Table C11.T2.

Table C11.T2. CND-A Position Requirements

CND-A	
Attribute	Level
Experience	Recommended at least 2 years of experience in CND technology or a related field.
System Environment	Works on a specific number of CND systems but analyzes events within the NE or enclave.
Knowledge	Significant knowledge of particular CND tools, tactics, techniques, and procedures which support their analysis of event information.
Supervision	Works under supervision and typically reports to a CND-SPM.
Other	Actions are usually authorized and controlled by policies and established procedures.
IAT-I or II <i>IA Baseline</i> Certification, CND <i>IA Baseline</i> Certification, and <i>CE/OS Certificate</i>	Within 6 months of assignment to position and mandatory for unsupervised privileged access.

C11.3.2. Table C11.T3. lists the specific functions associated with the CND-A position. Personnel performing these functions as their primary CND responsibilities, regardless of their occupational title within the CND-SP organization, shall be identified as part of the CND-A specialty and must comply with the requirements in Tables C11.T2. and C11.T3.



Table C11.T3. CND-A Functions

CND-A.1.	Mastery of IAT Level I and IAT Level II CE and/or NE knowledge and skills with applicable certification.
CND-A.2.	Receive and analyze network alerts from various sources within the NE or enclave and determine possible causes of such alerts.
CND-A.3.	Coordinate with enclave CND staff to validate network alerts.
CND-A.4.	Perform analysis of log files from a variety of sources within the NE or enclave, to include individual host logs, network traffic logs, firewall logs, and intrusion detection system logs.
CND-A.5.	Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.
CND-A.6.	Monitor external data sources (e.g. CND vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of CND threat condition and determine which security issues may have an impact on the NE or enclave.
CND-A.7.	Assist in the construction of signatures which can be implemented on CND network tools in response to new or observed threats within the NE or enclave.
CND-A.8.	Perform event correlation using information gathered from a variety of sources within the NE or enclave to gain situational awareness and determine the effectiveness of an observed attack.
CND-A.9.	Notify CND managers, CND incident responders, and other CND-SP team members of suspected CND incidents and articulate the event's history, status, and potential impact for further action.

C11.4. CND-IS

C11.4.1. CND-IS personnel test, implement, deploy, maintain, and administer the infrastructure systems which are required to effectively manage the CND-SP network and resources. This may include, but is not limited to routers, firewalls, intrusion detection/prevention systems, and other CND tools as deployed within the NE or enclave. Individuals within CND-SPs who maintain these infrastructure devices shall be considered CND-IS. CND-IS position requirements are listed in Table C11.T4.

Table C11.T4. CND-IS Position Requirements

CND-IS	
Attribute	Level
Experience	Recommended at least 4 years of experience in supporting CND and/or network systems and technology.
System Environment	Manages a number of specific CND tools/systems within the NE or enclave.
Knowledge	Significant knowledge of particular networking technologies, operating systems, and CND tools,

	tactics, techniques, and procedures which are part of the systems they support.
Supervision	Works under supervision and typically reports to a CND-SPM.
Other	Actions are usually authorized and controlled by policies and established procedures.
IAT-I or II <i>IA Baseline</i> Certification, CND <i>IA Baseline</i> Certification, and <i>CE/OS Certificate</i>	Within 6 months of assignment to position and mandatory for unsupervised privileged access. (Note CND-IS personnel supporting multiple systems must obtain the operating system certification for each system prior to getting full unsupervised privileged access. However, they may begin performing CND-IS duties on systems for which they do have OS certifications.)

C11.4.2. Table C11.T5. lists the specific functions associated with the CND-IS position. Personnel performing these functions as their primary CND responsibilities, regardless of their occupational title within the CND-SP organization, shall be identified as part of the CND-IS specialty and must comply with the requirements in Tables C11.T4. and C11.T5.

Table C11.T5. CND-IS Functions

CND-IS.1.	Mastery of the appropriate IAT Level I and IAT Level II CE and/or NE knowledge and skills with applicable certification.
CND-IS.2.	Create, edit, and manage changes to network access control lists on specialized CND systems (e.g., firewalls and intrusion prevention systems).
CND-IS.3.	Perform system administration on specialized CND applications and systems (e.g., anti-virus, or Audit/Remediation) to include installation, configuration, maintenance, and backup/restore.
CND-IS.4.	Implement C&A requirements for specialized CND systems within the NE or enclave, and document and maintain records for them.
CND-IS.5.	Coordinate with the CND-A to manage and administer the updating of rules and signatures (e.g., IDS/IPS, anti-virus, and content blacklists) for specialized CND applications.
CND-IS.6.	Identify potential conflicts with implementation of any CND tools within the CND-SP area of responsibility (e.g., tool/signature testing and optimization).
CND-IS.7.	Administer CND test bed and test and evaluate new CND applications, rules/signatures, access controls, and configurations of CND-SP managed platforms.

## C11.5. CND-IR

C11.5.1. CND-IR personnel investigate and analyze all response activities related to cyber incidents within the NE or Enclave. These tasks include, but are not limited to: creating and

maintaining incident tracking information; planning, coordinating, and directing recovery activities; and incident analysis tasks, including examining all available information and supporting evidence or artifacts related to an incident or event. Individuals within CND-SPs who perform any of the incident management and incident response tasks shall be considered CND-IRs. CND-IR position requirements are listed in Table C11.T6.

Table C11.T6. CND-IR Position Requirement

CND-IR	
Attribute	Level
Experience	Recommended at least 5 years of experience in CND technology or a related field.
System Environment	Works on a wide variety of systems within the NE or enclave as CND incidents dictate.
Knowledge	Significant knowledge of particular CND tools, tactics, techniques, and procedures which support the tracking, management, analysis, and resolution of incidents.
Supervision	Works under supervision and typically reports to a CND-SPM.
Other	Actions are usually authorized and controlled by policies and established procedures.
IAT-I, II, or III <i>IA Baseline</i> Certification, CND <i>IA Baseline</i> Certification, and <i>CE/OS Certificate</i>	Within 6 months of assignment to position and mandatory for unsupervised privileged access.

C11.5.2. Table C11.T7. lists the specific functions associated with the CND-IR position. Personnel performing these functions as their primary CND responsibilities, regardless of their occupational title within the CND-SP organization, shall be identified as part of the CND-IR specialty and must comply with the requirements in Tables C11.T.6. and C11.T7.

Table C11.T7. CND-IR Functions

CND-IR.1.	Mastery of the appropriate IAT Level I, IAT Level II, or IAT Level III CE, NE, or enclave knowledge and skills with applicable certification.
CND-IR.2.	Collect and analyze intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation potential CND incidents within the enclave.
CND-IR.3.	Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enclave systems.
CND-IR.4.	Coordinate with and provide expert technical support to enclave CND technicians to resolve CND incidents.

CND-IR.5.	Track and document CND incidents from initial detection through final resolution.
CND-IR.6.	Perform CND incident triage to include determining scope, urgency, and potential impact; identify the specific vulnerability and make recommendations which enable expeditious remediation.
CND-IR.7.	Correlate incident data and perform CND trend analysis and reporting.
CND-IR.8.	Coordinate with intelligence analysts to correlate threat assessment data.
CND-IR.9.	Serve as technical experts and liaisons to law enforcement personnel and explain incident details, provide testimony, etc.
CND-IR.10.	Perform real-time CND Incident Handling (e.g., forensic collections, intrusion correlation/tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRT).
CND-IR.11.	Maintain deployable CND toolkit (e.g., specialized CND software/hardware) to support IRT missions.
CND-IR.12.	Write and publish CND guidance and reports on incident findings to appropriate constituencies.

#### C11.6. CND-AU

C11.6.1. CND-AU personnel perform assessments of systems and networks within the NE or enclave and identify where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. CND-AUs achieve this through passive evaluations (compliance audits) and active evaluations (penetration tests and/or vulnerability assessments). Individuals within CND-SPs who perform compliance and audit related tasks shall be considered CND-AUs. CND-AU position requirements are listed in Table C11.T8.

Table C11.T8. CND-AU Position Requirements

CND-AU	
Attribute	Level
Experience	Recommended at least 2 years of experience in CND technology or a related field.
System Environment	Works on a specific number of CND systems but does compliance testing on portions of the NE or enclave.
Knowledge	Significant knowledge of particular CND tools, tactics, techniques, and procedures which support their compliance tests.
Supervision	Works under supervision and typically reports to a CND Manager.
Other	Actions are usually authorized and controlled by policies and established procedures.
IAT-I, II, or III <i>IA Baseline</i> Certification,	Within 6 months of assignment to position and mandatory for unsupervised privileged access.

CND <i>IA Baseline</i> Certification, and <i>CE/OS Certification</i> <i>Certificate</i>	
--	--

C11.6.2. Table C11.T9. lists the specific functions associated with the CND-AU position. Personnel performing these functions as their primary CND responsibilities, regardless of their occupational title within the CND-SP organization, shall be identified as part of the CND-AU specialty and must comply with the requirements in the Tables C11.T8. and C11.T9.

Table C11.T9. CND-AU Functions

CND-AU.1.	Mastery of the appropriate IAT Level I, IAT Level II, or IAT Level III CE, NE, or enclave knowledge and skills with applicable certification.
CND-AU.2.	Maintain knowledge of applicable CND policies, regulations, and compliance documents specifically related to CND auditing.
CND-AU.3.	Perform CND vulnerability assessments within the enclave.
CND-AU.4.	Perform CND risk assessments within the enclave.
CND-AU.5.	Conduct authorized penetration testing of enclave network assets.
CND-AU.6.	Analyze site/enclave CND policies and configurations and evaluate compliance with regulations and enclave directives.
CND-AU.7.	Prepare audit reports that identify technical and procedural findings and provide recommended remediation strategies/solutions.
CND-AU.8.	Maintain deployable CND audit toolkit (e.g., specialized CND software/hardware) to support CND audit missions.

C11.7. CND-SPM

C11.7.1. CND-SPMs oversee the CND-SP operations within their organization. CND-SPMs are responsible for producing guidance for their NE or enclave, assisting with risk assessments and risk management for organizations within their NE or enclave, and are responsible for managing the technical classifications within their organization. CND-SPM position requirements are listed in Table C11.T10.

Table C11.T10. CND-SPM Position Requirements

CND-SPM	
Attribute	Level
Experience	Recommended at least 4 years of experience in CND management or a related field.
System Environment	Manages technicians who are responsible for all CND duties across the entire NE or enclave.
Knowledge	Significant knowledge of the capabilities and limitations of particular CND tools, tactics, techniques, and procedures which are employed by the technicians within the NE or enclave.

Supervision	Supervises technicians within the organization; reports to a senior CND Manager or to USSTRATCOM.
Other	Actions are usually authorized and controlled by policies and established procedures.
IAM-I or II <i>IA Baseline</i> Certification and CND <i>IA Baseline</i> Certification	Within 6 months of assignment to position and mandatory for unsupervised privileged access.

C11.7.2. Table C11.T11. lists the specific functions associated with the CND-SPM position. Personnel performing these functions as their primary CND responsibilities, regardless of their occupational title within the CND-SP organization, shall be identified as part of the CND-SPM specialty and must comply with the requirements in Tables C11.T10. and C11.T11.

Table C11.T11. CND-SPM Functions

CND-SPM.1. Mastery of the appropriate IAM Level I or IAM Level II CE and/or NE knowledge and skills with applicable certification.
CND-SPM.2. Implement and enforce CND policies and procedures reflecting applicable laws, policies, procedures, and regulations (e.g., Reference ( <i>gi</i> )).
CND-SPM.3. Manage the publishing of CND guidance (e.g., IAVAs and TCNOs) for the enclave constituency.
CND-SPM.4. Provide incident reports, summaries, and other situational awareness information to higher headquarters.
CND-SPM.5. Manage an incident (e.g., coordinate documentation, work efforts, resource utilization within the organization) from inception to final remediation and after action reporting.
CND-SPM.6. Manage threat or target analysis of CND information and production of threat or target information within the network or enclave environment.
CND-SPM.7. Manage the monitoring of external CND data sources to maintain enclave situational awareness.
CND-SPM.8. Interface with external organizations (e.g., public affairs, law enforcement, Command or Component Inspector General) to ensure appropriate and accurate dissemination of incident and other CND information.
CND-SPM.9. Lead risk analysis and management activities for the network or enclave environment.
CND-SPM.10. Track compliance audit findings, incident after-action reports, and recommendations to ensure appropriate mitigation actions are taken.

## AP1. APPENDIX 1

### DEFINITIONS

#### AP1. DEFINITIONS

AP1.1. Authorized User. As defined in Reference (a), any appropriately cleared individual required to access a DoD IS to carry out or assist in a lawful and authorized governmental function. Authorized users include: DoD employees, contractors, and guest researchers.

AP1.2. Categories, Specialties, Levels, and Functions. As defined in Reference (a), the structure for identifying all DoD Information Assurance (IA) positions and personnel.

AP1.2.1. Categories, Specialties. The DoD IA workforce is split into two major categories of Technical and Management. Management refers to personnel performing any IAM functions described in Chapters 4 or 5. Specialties are a category of the DoD IA Workforce performing advanced and/or specialized functions. Specialties may perform functions at various levels. A specialty may also require the mastery of a specified Technical or Management level.

AP1.2.2. Levels. Each of the IA workforce categories has three levels (Technical or Management Level I, II, and III). The management category also includes the Designated Accrediting Authority (DAA) position.

AP1.2.3. Functions. High level tasks required to successfully perform IA for an information system. The function indicates the tasks that an employee performs or occupational requirements to successfully perform as part of the IA Workforce. For the purposes of this Manual the IA functions have been associated with a category and level. These functions provide a means to distinguish between different levels of work. The functional level approach also encourages a broader, more integrated means of identifying what an employee must know to perform the tasks that comprise an IA position across all of the DoD Components.

AP1.3. Certification. Recognition given to individuals who have met predetermined qualifications set by an agency of government, industry, or profession. Certification provides verification of individuals' knowledge and experience through evaluation and approval, based on a set of standards for a specific profession or occupation's functional job levels. Each certification is designed to stand on its own, and represents an individual's mastery of a particular set of knowledge and skills.

AP1.4. Computing Environment (CE). Per Reference (~~h~~), local area network(s) server host and its operating system, peripherals, and applications.

AP1.5. Contractor. Per the Defense Acquisition University Glossary, "an entity in private industry which enters into contracts with the government to provide goods or services." For DoD IA purposes, an entity is a private sector employee performing IA functions in support of a



DoD IS. Private sector employees performing IA functions must meet the same standards for system access or management as government IA employees.

AP1.6. Defense Civilian Personnel Data System (DCPDS). DCPDS is a human resources transaction IS supporting civilian personnel operations in the Department of Defense. DCPDS is designed to support appropriated fund, non-appropriated fund, and LN human resources operations.

AP1.6.1. The Corporate Management Information System (CMIS) consolidates DoD employee and position data for all DoD civilian employees from all DCPDS databases to provide a corporate level data query and reporting capability.

AP1.6.2. DCPDS and CMIS support strategic DoD civilian workforce planning, trend analysis, mobilization, and contingency planning.

AP1.7. Designated Accrediting Authority (DAA). As defined in Reference (b).

AP1.8. DoD Information System (IS). As defined in References (a) and (b), includes automated IS (AIS) applications, enclaves, outsourced IT based processes, and platform IT interconnections.

AP1.8.1. An AIS application performs clearly defined functions for which there are readily identifiable security considerations and needs addressed as part of the acquisition. An AIS application may be a single software application (e.g., Integrated Consumable Items Support); multiple software applications related to a single mission (e.g., payroll or personnel); or a combination of software and hardware performing a specific support function across a range of missions (e.g., Global Command and Control System, Defense Messaging System ). AIS applications are deployed to enclaves for operations and have their operational security needs assumed by the enclave.

AP1.8.2. Note: An AIS application is analogous to a “major application,” as defined in OMB A-130 (Reference (1n)). However, to avoid confusion with the DoD acquisition category called “Major Automated Information System”, this term (AIS) is not used in this Manual.

AP1.9. Duty.

AP1.9.1. Primary. An IA position with primary duties focused on IA functions. The position may have other duties assigned, but the main effort focuses on IA functions. The position would normally require at least 25 to 40(+) hours per week devoted to IA functions.

AP1.9.2. Additional. A position requiring a significant portion of the incumbent’s attention and energies to be focused on IA functions, but in which IA functions are not the primary responsibility. The position would normally require 15 to 24 hours, out of a 40(+) hour week, devoted to IA functions.



AP1.9.3. Embedded. A position with IA functions identified as an integral part of other major assigned duties. These positions normally require up to 14 hours, out of a 40(+) hour week be devoted to IA related functions.

AP1.10. Eligible DoD Contractors. An employee or individual under contract or subcontract to the Department of Defense, designated as providing services or support to the Department that requires logical and/or physical access to the Department's assets.

AP1.11. Enclave. As defined in Reference (~~f~~h) a collection of CE connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves provide standard IA capabilities such as boundary defense, incident detection and response, and key management, and also deliver common applications such as office automation and electronic mail. Enclaves are analogous to general support systems, as defined in OMB A-130 (Reference (~~h~~)). Enclaves may be specific to an organization or a mission and the CE may be organized by physical proximity or by function, independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers.

AP1.12. Foreign National. Individuals who are non-U.S. citizens including U.S. military personnel, DoD civilian employees, and contractors.

AP1.13. General Schedule (GS)/Pay Band. The Office of Personnel Management's basic classification and compensation system for white collar occupations in the federal government, as established by Reference (~~w~~y).

AP1.13.1. Job Series. A subgroup of an occupational group or job family that includes all classes of positions at the various levels in a particular kind of work, such as the GS-2210 series. Positions within a series are similar in subject matter, basic knowledge and skill requirements.

AP1.13.2. Parenthetical Specialty. A subset of work within a series distinguishing positions on the basis of specialized technical requirements. For example, the 2210 series has officially designated parenthetical specialties agencies must include in the official position titles. "INFOSEC" is the parenthetical specialty used in DCPDS for 2210 employees performing security (IA) functions.

AP1.13.3. Position Specialty Code. A unique DoD civilian workforce code to support effective management of the IA workforce. The position specialty code identifies a DoD civilian position, or person with IA functions, regardless of OPM job series.

AP1.14. Information Assurance (IA). Per Reference (~~f~~h), measures that protect and defend information and ISs by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of IS by incorporating protection, detection, and reaction capabilities.

AP1.15. Information Assurance Workforce. The IA workforce focuses on the operation and management of IA capabilities for DoD systems and networks. The workforce ensures adequate security measures and established IA policies and procedures are applied to all ISs and networks. The IA workforce includes anyone with privileged access and IA managers who perform any of the responsibilities or functions described in Chapters 3-5,10 or 11. The DoD IA Workforce includes but is not limited to all individuals performing any of the IA functions described in this Manual. Additionally the IA workforce categories, specialties and their /functions will be expanded to include for example system architecture and engineering, and computer network defense, certification and accreditation, and vulnerability assessment as changes to this Manual. These individuals are considered to have significant “security responsibilities” and must receive specialized training and be reported per Reference (c) and this Manual.

AP1.16. Information Assurance Vulnerability Alert (IAVA). The comprehensive distribution process for notifying the Components about vulnerability alerts and countermeasures information as established in Reference (g).

AP1.17. Information Assurance Vulnerability Management (IAVM). The IAVM process provides positive control of the vulnerability notification process for DoD network assets. The IAVM requires Components receipt acknowledgement and provides specific time parameters for implementing appropriate countermeasures, depending on the criticality of the vulnerability.

AP1.18. Information Operations Condition (INFOCON). A comprehensive defense posture and response based on the status of ISs, military operations, and intelligence assessments of adversary capabilities and intent.

AP1.19. Local National Employee. Per Reference (a) civilians or contractors, whether paid from appropriated or non-appropriated funds, employed or used by the U.S. Forces in a foreign country who are nationals or non-U.S. residents of that country.

AP1.20. Network Environment (Computer). The constituent element of an enclave responsible for connecting CE by providing short haul data transport capabilities, such as local or campus area networks, or long haul data transport capabilities, such as operational, metropolitan, or wide area and backbone networks that provides for the application of IA controls.

AP1.21. Network Operations. An organizational and procedural framework intended to provide DoD IS and computer network owners the means to manage their systems and networks. This framework allows IS and computer network owners to effectively execute their mission priorities, support DoD missions, and maintain the IS and computer networks. The framework integrates the mission areas of network management, information dissemination management, and information assurance.

AP1.22. Privileged Access. An authorized user who has access to system control, monitoring, administration, criminal investigation, or compliance functions. Privileged access typically provides access to the following system controls:

AP1.22.1. Access to the control functions of the information system/network, administration of user accounts, etc.

AP1.22.2. Access to change control parameters (e.g., routing tables, path priorities, addresses) of routers, multiplexers, and other key information system/network equipment or software.

AP1.22.3. Ability and authority to control and change program files, and other users' access to data.

AP1.22.4. Direct access to operating system level functions (also called unmediated access) that would permit system controls to be bypassed or changed.

AP1.22.5. Access and authority for installing, configuring, monitoring, or troubleshooting the security monitoring functions of information systems/networks (e.g., network/system analyzers; intrusion detection software; firewalls) or in performance of cyber/network defense operations.

AP1.23. Red Team. An independent and focused threat based effort by a multi-disciplinary, opposing force using active and passive capabilities; based on formal; time bounded tasking to expose and exploit information operations vulnerabilities of friendly forces as a means to improve readiness of U.S. units, organizations, and facilities.

AP1.24. Supporting IA Infrastructures. Collections of interrelated processes, systems, and networks providing a continuous flow of information assurance services throughout the Department of Defense (e.g., the key management infrastructure or the incident detection and response infrastructure).

AP1.25. Training.

AP1.25.1. Resident. Instructor led classroom instruction based on specific performance criteria.

AP1.25.2. Distributive. Computer based training (CBT) via website, computer disc, or other electronic media.

AP1.25.3. On the job training (OJT). Supervised hands on training, based on specific performance criteria that must be demonstrated to a qualified supervisor.

AP1.25.4. Blended: A combination of instructor led classroom training and distributed media. This may also include instructor led classroom training using distributed multi-media.

AP1.26. Waivers.

AP1.26.1. DAAs may waive the IAT or IAM certification requirement(s) under severe operational or personnel constraints. The waiver must be documented by the DAA using a memorandum for the record stating the reason for the waiver and the plan to rectify the constraint. Waivers must be time limited, not to exceed six months, and include an expiration date. Uncertified IAT Level Is are not authorized unsupervised privileged access until fully qualified per Chapter 3.

AP1.26.2. Waivers for IAT Level I certification requirements are not authorized for personnel deployed to a combat theatre of operations. The DAA may approve a waiver for certified IAT-Is to fill level IAT-II or IAT-III billets while deployed in a combat environment without attaining the appropriate certification. The DAA may grant an interim waiver limited to the period of the deployment. The interim waiver places an individual in a suspense status and must be time limited and include an expiration date not to exceed six months following date of return from combat status. The DAA may also authorize waivers for certified IAM-Is or IAM IIs to fill higher management positions in combat zones.

## APPENDIX 2

### AP2. IA WORKFORCE LEVELS, FUNCTIONS, AND CERTIFICATION APPROVAL PROCESS

#### AP2.1. CERTIFICATION CRITERIA

AP2.1.1. The list of certifications ~~contained in Table AP3.T2~~ *posted on the DISA IASE website* (<http://iase.disa.mil/eta/iawip/>) is approved for the DoD IA workforce as of the publication date of *Change 3* to this Manual.

AP2.1.2. The ~~table list of certifications~~ map ~~the~~ to the IA categories, specialties and levels to which they apply.

AP2.1.2.1. IA personnel must obtain and maintain a certification corresponding to the highest level function(s) they perform. Certifications held by an IA workforce member on the “change date” to this Manual remain valid for as long as member remains in that position and keeps their certification status up to date according to individual certification provider standards.

AP2.1.2.2. Individuals performing IAT functions must hold, at a minimum, an IAT Level I certification, before gaining privileged access to any DoD system.

AP2.1.2.3. Individuals performing functions in multiple categories or specialties must hold certifications appropriate to the functions performed in each category or specialty.

AP2.1.3. Commercial, vendor specific, or component developed equivalent certifications approved for the DoD IA workforce requirement must align to the IA category or specialty functional requirements. For validity, certifications must be accredited and maintain accreditation through the American National Standards Institute (ANSI) under the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 17024, “General Requirements for Bodies Operating Certification of Persons,” April 2003 ISO/IEC 17024 Standard, Reference (~~xz~~). ANSI is the only personnel certification accreditation body in the United States to meet ISO/IEC 17011:2004, "Conformity assessment - General requirements for accreditation bodies accrediting conformity assessment bodies" (Reference (~~yz~~)), which represents the highest nationally accepted practices for accreditation bodies. Certifications that receive ANSI accreditation also must be approved by the IA WIPAC for inclusion into this Manual as a baseline certification.

#### AP2.2. CERTIFICATION REVIEW PROCESS

AP2.2.~~21~~. The Office of the DoD ~~DCIO~~ will charter and chair the IA WIPAC to maintain the workforce categories, levels, functions, and certifications. The IA WIPAC must meet periodically to approve, remove and assign certifications to the appropriate IA workforce levels.

*All changes to the approved IA baseline certification list will be made or vetted by the IA WIPAC. The DISA IASE website will be updated to reflect the IA WIPAC's changes.*

AP2.2.12. The list of approved IA *baseline* certifications must be reviewed at least annually to ensure continued applicability to the Department of Defense. Certifications may be government or commercially granted, but *all IA baseline certifications* must be accredited *through ANSI* to the requirements of Reference (xz) *prior to being considered by the IA WIPAC for addition to the approved IA baseline certification list.* ~~Certifications listed in this Manual currently do not all meet this standard. Each has submitted a letter of intent to do so within two years from the publication date of this Manual. Certifications not accredited through ANSI to the ISO standard within two years cannot be used to meet the DoD IA security standard. However, they may, if appropriate, be used to meet Component local operating system requirements.~~

~~AP2.2.3. Appendix 3 will be updated and reissued as needed to reflect the results of this review process.~~

AP3. APPENDIX 3IA WORKFORCE REQUIREMENTS AND CERTIFICATIONS

AP3.1 Table AP3.T1 consolidates IA workforce requirements described in this Manual. Requirements for each category are discussed and described in more depth in the preceding chapters of this Manual.

Table AP3.T1 Summary of IA Workforce Requirements

	IAT I-III	IAM I-III	IASAE I-III	CND-A, CND-IS, CND-IR, CND-AU and CND-SPM
Initial Training	Yes* <del>※</del>	Yes* <del>※</del>	Yes* <del>※</del>	Yes* <del>※</del>
<i>IA Baseline</i> Certification (from approved list)	Yes (IA Certification) (within 6 months)	Yes (IA Certification) (within 6 months)	Yes (IA Certification) (within 6 months)	Yes (CND Certification) (within 6 months)
<i>Initial</i> OJT Evaluation	Yes (for initial position)	No	No	Yes (except CND-SPM)
<i>CE/OS</i> <del>Certification</del> <i>Certificate</i>	Yes	No	No	Yes (except CND-SPM)
Maintain Certification Status	Yes (as required by certification)	Yes (as required by certification)	Yes (as required by certification)	Yes (as required by certification)
Continuous Education or Sustainment Training	Yes (as required by certification)	Yes (as required by certification)	Yes (as required by certification)	Yes (as required by certification)
Background Investigation	As required by IA level and Reference (b)	As required by IA level and Reference (b)	As required by IA level and Reference (b)	As required by CND-SP level and Reference (b)
Sign Privileged Access Statement	Yes	n/a	n/a	Yes
Experience	IAT I: Normally has 0 to 5 or more years of experience in IA technology or a related field.	IAM I: Usually an entry level management position with 0 to 5 or more years of management experience.	IASAE I: Usually an entry level IASAE position with 0 or more years of IASAE experience.	Recommended years of experience in CND technology or a related field: CND-A: at least 2 CND-IR: at least 5 CND-AU: at least 2
	IAT II: Normally has at least 3 years in IA technology or a related area.	IAM II: Usually has at least five years of management experience.	IASAE II: Usually has at least 5 years of IASAE experience.	CND-IS: Recommended at least 4 years of experience supporting CND and/or network systems and technology

	IAT III: Normally has at least seven years experience in IA technology or a related area.	IAM III: Usually has at least 10 years of management experience.	IASAE III: Usually has at least 10 years of IASAE experience.	CND-SPM: Recommended at least 4 years of experience in CND management or a related field
*Classroom, distributive, blended or commercial provider				
**Classroom, distributive, blended, government or commercial provider				

AP3.2. ~~Each cell within Table AP3.T2~~ *The approved IA baseline certifications table on the DISA IASE website* (<http://iase.disa.mil/eta/iawip/>) provides a list of DoD approved certifications aligned to each category and level of the IA Workforce. Personnel performing IA functions must obtain one of the certifications required for their positions category or specialty and level. DoD Components may choose any approved certification to meet the certification requirements for the associated level for which the certification has been approved.

AP3.2.1. ~~Each cell within Table AP3.T3 contains~~ *The IASE website lists* the names of the organizations that ~~sponsors the own each~~ certification. These may be commercial, government, or other entities whose certification meets the requirements for the IA functional level(s) represented by the cell.

AP3.2.2. A certification may apply to more than one level.

AP3.2.3. Most IA levels within a category or specialty have more than one approved certification.

AP3.2.4. An individual needs to obtain only one of the “approved certifications” for his or her IA category or specialty and level to meet the minimum requirement. For example, an individual in an IAT Level II position could obtain any one of the four certifications listed in the corresponding cell.

AP3.2.4.1. Higher level IAT certifications satisfy lower level requirements. Certifications listed in Level II or III cells can be used to qualify for Level I. However, Level I certifications cannot be used for Level II or III unless the certification is also listed in the Level II or III cell. For example:

AP3.2.4.1.1. The A+ or Network+ certification qualify only for Technical Level I and cannot be used for Technical Level II positions.

AP3.2.4.1.2. The System Security Certified Practitioner (SSCP) certification qualifies for both Technical Level I and Technical Level II. If the individual holding this certification moved from an IAT Level I to an IAT Level II position, he or she would not have to take a new certification.

AP3.2.5. Higher-level IAM certifications satisfy lower level requirements. Certifications listed in Level II or III cells can be used to qualify for Level I. However, Level I certifications cannot be used for Level II or III unless the certification is also listed in the Level II or III cell.



AP3.2.6. Operating System Requirement. IATs and designated CND-SPs must also obtain certifications required to implement the IA requirements for their specific operating system environment (e.g., Microsoft Operating Systems Administrator Certification), unless the operating system certification is also on the list of approved DoD IA *baseline* certifications. ~~at~~ **Table AP3.T2**

*AP3.2.7. All IA workforce personnel must maintain their certifications as required by their certification providers to retain their DoD IA workforce position.*

*AP3.2.8. Changes to the approved IA baseline certification list will be made by the IA WIPAC in accordance with AP2.2.1. The DISA IASE website will be updated to reflect these changes.*

AP3.3. ~~Each cell within Table AP3.T2.~~*The approved IA baseline certification table on the DISA IASE website* (<http://iase.disa.mil/eta/iawip/>) provides a list of DoD approved certifications for personnel performing IA functions that meet baseline requirements. DoD Components may choose any of the approved certifications to meet the applicable certification requirements for each associated level.

~~Table AP3. T2. DoD Approved Baseline Certifications~~

---

Table AP3.T3. IA Workforce Certification Organizations

Certification Provider	Certification Name
Carnegie Mellon Software Engineering Institute CERT®*	Computer Security Incident Handler (CSIH)
Computing Technology Industry Association (CompTIA) *	A+
CompTIA*	Security+
CompTIA*	Network+
EC Council*	Certified Ethical Hacker (CEH)
International Information Systems Security Certifications Consortium (ISC)2*	Certified Information Systems Security Professional (CISSP) (or Associate—this means the individual has qualified for the certification except for the number of years experience)
(ISC)2*	Certification and Accreditation Professional (CAP)
(ISC)2*	Information Systems Security Architecture Professional (ISSAP)
(ISC)2*	Information Systems Security Engineering Professional (ISSEP)
(ISC)2*	Information Systems Security Management Professional (ISSMP)
(ISC)2*	System Security Certified Practitioner (SSCP)
Information Systems Audit and Control Association (ISACA) *	Certified Information Security Manager (CISM)
ISACA*	Certified Information Security Auditor (CISA)
SecurityCertified Program*	Security Certified Network Professional (SCNP)
SecurityCertified Program*	Security Certified Network Architect (SCNA)
Global Information Assurance Certification (GIAC) *	GIAC Certified Intrusion Analyst (GCIA)
GIAC*	GIAC Certified Incident Handler (GCIH)
GIAC*	GIAC Security Expert (GSE)
GIAC*	GIAC Security Essentials Certification (GSEC)
GIAC*	GIAC Security Leadership Certificate (GSLC)
GIAC*	GIAC Systems and Network Auditor (GSNA)
GIAC*	GIAC Information Security Fundamentals (GISF)
* This organization is the sole propriety owner of the memberships, site licenses, preassessments, test vouchers, and all other materials related to this certification and their association.	

APPENDIX 4

AP4. SAMPLE STATEMENT OF ACCEPTANCE OF RESPONSIBILITIES

<IS NAME>

INFORMATION SYSTEM PRIVILEGED ACCESS AGREEMENT AND  
ACKNOWLEDGMENT OF RESPONSIBILITIES

Date: \_\_\_\_\_

1. I understand there are two DoD Information Systems (IS), classified (SIPRNET) and unclassified (NIPRNET), and that I have the necessary clearance for privileged access to <IS NAME> [specify which IS the privileges are for]. I will not introduce or process data or software for the IS that I have not been specifically authorized to handle.
2. I understand the need to protect all passwords and other authenticators at the highest level of data they secure. I will not share any password(s), account(s), or other authenticators with other coworkers or other personnel not authorized to access the < IS NAME>. As a privileged user, I understand the need to protect the root password and/or authenticators at the highest level of data it secures. I will NOT share the root password and/or authenticators with coworkers who are not authorized <IS NAME > access.
3. I understand that I am responsible for all actions taken under my account(s), root, or otherwise. I will not attempt to “hack” the network or any connected information systems, or gain access to data to which I do not have authorized access.
4. I understand my responsibility to appropriately protect and label all output generated under my account (including printed materials, magnetic tapes, floppy disks, and downloaded hard disk files).
5. I will immediately report any indication of computer network intrusion, unexplained degradation or interruption of network services, or the actual or possible compromise of data or file access controls to the appropriate <IS NAME > Information Assurance Management (IAM) or senior Information Assurance Technical (IAT) Level representatives. I will NOT install, modify, or remove any hardware or software (e.g., freeware/shareware and security tools) without written permission and approval from the <IS NAME > IAM-or senior IAT Level representatives.
6. I will not install any unauthorized software (e.g., games, entertainment software) or hardware (e.g., sniffers).
7. I will not add/remove any users’ names to the Domain Administrators, Local Administrator, or Power Users group without the prior approval and direction of the <IS NAME > IAM/or senior IAT Level representatives.

8. I will not introduce any unauthorized code, Trojan horse programs, malicious code, or viruses into the <IS NAME > local area networks.

9. I understand that I am prohibited from the following while using the DoD IS:

a. Introducing Classified and/or Controlled Unclassified Information (CUI) into a NIPRNet environment.

b. Accessing, storing, processing, displaying, distributing, transmitting, or viewing material that is abusive, harassing, defamatory, vulgar, pornographic, profane, or racist; that promotes hate crimes, or is subversive or objectionable by nature, including material encouraging criminal activity, or violation of local, state, federal, national, or international law.

c. Storing, accessing, processing, or distributing Classified, Proprietary, CUI, For Official Use Only (FOUO), or Privacy Act protected information in violation of established security and information release policies.

d. Obtaining, installing, copying, pasting, transferring, or using software or other materials obtained in violation of the appropriate vendor's patent, copyright, trade secret, or license agreement.

e. Knowingly writing, coding, compiling, storing, transmitting, or transferring malicious software code, to include viruses, logic bombs, worms, and macro viruses.

f. Engaging in prohibited political activity.

g. Using the system for personal financial gain such as advertising or solicitation of services or sale of personal property (e.g., eBay), or stock trading (i.e., issuing buy, hold, and/or sell directions to an online broker).

h. Fundraising activities, either for profit or non-profit, unless the activity is specifically approved by the organization (e.g., organization social event fund raisers and charitable fund raisers, without approval).

i. Gambling, wagering, or placing of any bets.

j. Writing, forwarding, or participating in chain letters.

k. Posting personal home pages.

l. Any other actions prohibited by DoD 5500.7-R (Reference (~~y~~aa)) or any other DoD issuances.

10. Personal encryption of electronic communications is strictly prohibited and can result in the immediate termination of access.

11. I understand that if I am in doubt as to any of my roles or responsibilities I will contact the <IS NAME > IAT Level III Supervisor for clarification.
12. I understand that all information processed on the <IS NAME> is subject to monitoring. This includes email and browsing the web.
13. I will not allow any user who is not cleared access to the network or any other connected system without prior approval or specific guidance from the <IS NAME> IAM.
14. I will use the special access or privileges granted to me ONLY to perform authorized tasks or mission related functions.
15. I will not use any <DOD/Components> owned information system to violate software copyright by making illegal copies of software.
16. I will ONLY use my PRIVILEGED USER account for official administrative actions. This account will NOT be used for day to day network communications.
17. I understand that failure to comply with the above requirements will be reported and may result in the following actions:
  - a. Revocation of IS privileged access.
  - b. Counseling.
  - c. Adverse actions pursuant to the Uniform Code of Military Justice and/or criminal prosecution.
  - d. Disciplinary action, discharge or loss of employment.
  - e. Revocation of Security Clearance.
18. I will obtain and maintain required certification(s), according to DoD 8570.01-M and the certification provider, to retain privileged system access.

YOUR IAT Level III Supervisor is \_\_\_\_\_

INFORMATION SYSTEM NAME \_\_\_\_\_

IAT/IASAE/CND's NAME \_\_\_\_\_

IAT/IASAE/CND's SIGNATURE \_\_\_\_\_

Date \_\_\_\_\_

IAM LEVEL I NAME \_\_\_\_\_

IAM LEVEL I SIGNATURE \_\_\_\_\_

Date\_\_\_\_\_

(Level I or II Managers with privileged access will have signatures of the IAM Level II or III responsible for their IS functions).



# Department of Defense **INSTRUCTION**

**NUMBER 8510.01**  
November 28, 2007

---

---

ASD(NII)/DoD CIO

**SUBJECT:** DoD Information Assurance Certification and Accreditation Process (DIACAP)

**References:** (a) Subchapter III of Chapter 35 of title 44, United States Code, "Federal Information Security Management Act (FISMA) of 2002"  
(b) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002  
(c) DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002  
(d) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003  
(e) through (ab), see Enclosure 1

## 1. PURPOSE

This Instruction:

1.1. Implements References (a), (b), (c), and (d) by establishing the DIACAP for authorizing the operation of DoD Information Systems (ISs).

1.2. Cancels DoD Instruction (DoDI) 5200.40; DoD 8510.1-M; and ASD(NII)/DoD CIO memorandum, "Interim Department of Defense (DoD) Information Assurance (IA) Certification and Accreditation (C&A) Process Guidance" (References (e), (f), and (g)).

1.3. Establishes or continues the following positions, panels, and working groups to implement the DIACAP: the Senior Information Assurance Officer (SIAO), the Principal Accrediting Authority (PAA), the Defense Information Systems Network (DISN)/Global Information Grid (GIG) Flag Panel, the IA Senior Leadership (IASL), the Defense (previously DISN) IA Security Accreditation Working Group (DSAWG), and the DIACAP Technical Advisory Group (TAG).

1.4. Establishes a C&A process to manage the implementation of IA capabilities and services and provide visibility of accreditation decisions regarding the operation of DoD ISs, including core enterprise services- and Web services-based software systems and applications.



1.5. Prescribes the DIACAP to satisfy the requirements of Reference (a) and requires the Department of Defense to meet or exceed the standards required by the Office of Management and Budget (OMB) and the Secretary of Commerce, pursuant to Reference (a) and section 11331 of title 40, United States Code (Reference (h)).

## 2. APPLICABILITY AND SCOPE

2.1. This Instruction applies to:

2.1.1. The Office of the Secretary of Defense (OSD), the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General (IG) of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as the “DoD Components”).

2.1.2. DoD-owned ISs and DoD-controlled ISs operated by a contractor or other entity on behalf of the Department of Defense that receive, process, store, display, or transmit DoD information, regardless of classification or sensitivity, consistent with Reference (b).

2.2. Nothing in this Instruction shall alter or supersede the existing authorities and policies of the Director of National Intelligence regarding the protection of Sensitive Compartmented Information (SCI) and special access programs for intelligence as directed by Executive Order 12333 (Reference (i)) and other laws and regulations. The application of the provisions and procedures of this Instruction to SCI or other intelligence ISs is encouraged where they may complement or discuss areas not otherwise specifically addressed.

## 3. DEFINITIONS

Terms used in this Instruction are defined in Enclosure 2.

## 4. POLICY

It is DoD policy that:

4.1. The Department of Defense shall certify and accredit ISs through an enterprise process for identifying, implementing, and managing IA capabilities and services. IA capabilities and services are expressed as IA controls as defined in Reference (d). IA controls are maintained through a DoD-wide configuration control and management (CCM) process that considers the GIG architecture and risk assessments that are conducted at DoD-wide, mission area (MA), DoD Component, and IS levels consistent with Reference (a).

4.2. The Department of Defense shall establish and use an enterprise decision structure for IA C&A that includes and integrates GIG MAs pursuant to DoD Directive (DoDD) 8115.01 (Reference (j)) and the DIACAP governance process prescribed in this Instruction.

4.3. The DIACAP shall support the transition of DoD ISs to GIG standards and a net-centric environment while enabling assured information sharing by:

4.3.1. Providing a standard C&A approach.

4.3.2. Providing guidance on managing and disseminating enterprise standards and guidelines for IA design, implementation, configuration, validation, operational sustainment, and reporting.

4.3.3. Accommodating diverse ISs in a dynamic environment.

4.4. All DoD-owned or -controlled ISs shall be under the governance of a DoD Component IA program in accordance with Reference (d). The DoD Component IA program shall be the primary mechanism for ensuring enterprise visibility and synchronization of the DIACAP.

4.5. All DoD ISs shall be implemented using the baseline DoD IA controls in accordance with Reference (d). The baseline DoD IA controls may be augmented if required to address localized threats or vulnerabilities.

4.6. A DIACAP Scorecard with a manual or DoD Public Key Infrastructure (PKI)-certified digital signature shall be visible to the DoD Chief Information Officer (CIO) and the DoD Component CIOs. The DIACAP Scorecard shall document the designated accrediting authority (DAA) accreditation decision as well as the results of the implementation of required baseline IA controls and additional IA controls that may be required by the DoD Component or local IS.

4.7. An Information Technology (IT) Security Plan of Action and Milestones (POA&M) shall be developed and maintained to record the status of any corrective actions directed in association with an accreditation decision.

4.8. The accreditation status and supporting DIACAP Package of DoD ISs shall be made available to interconnecting ISs, if requested, to support DAA accreditation decisions and to the Office of the IG DoD for audit and Federal Information Security Management Act (FISMA) assessment purposes.

4.9. All DoD ISs with an authorization to operate (ATO) shall be reviewed annually to confirm that the IA posture of the IS remains acceptable. Reviews will include validation of IA controls and be documented in writing.

4.10. Resources for implementing the DIACAP shall be identified and allocated as part of the Defense planning, programming, budgeting, and execution process.

4.11. Contracts for systems, services, and programs covered by this Instruction shall include clauses requiring compliance with the DIACAP. Failure to include such clauses is not justification for DIACAP non-compliance.

## 5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Networks and Information Integration/DoD CIO (ASD(NII)/DoD CIO) shall:

5.1.1. Oversee implementation of this Instruction, distribute DIACAP information standards and sharing requirements, and manage the transition from the previous DoD C&A process (Reference (e)) to the DIACAP.

5.1.2. Conduct an annual assessment of DoD Component IA programs for presentation in the annual report to Congress required by Reference (a).

5.1.3. Appoint a PAA for DoD ISs governed by the Enterprise Information Environment MA (EIEMA).

5.1.4. Appoint a DoD SIAO corresponding to a senior agency information security officer in Reference (a).

5.1.5. Provide annual certification to the Secretary of Defense and Director of OMB confirming that the DIACAP process is current and more stringent than the standards required by the OMB and the Secretary of Commerce pursuant to Reference (a).

5.2. The DoD SIAO, under the authority, direction, and control of the ASD(NII)/DoD CIO, shall direct and coordinate the DoD IA Program (Reference (d)) and:

5.2.1. Ensure DoD ISs are assigned to and governed by a DoD Component IA program.

5.2.2. Advise, inform, and support the GIG PAAs and their representatives.

5.2.3. Establish and maintain a DIACAP CCM process, a DIACAP TAG, and an online DIACAP Knowledge Service (KS).

5.3. The Director, Defense Information Systems Agency (DISA), under the authority, direction, and control of the ASD(NII)/DoD CIO, shall:

5.3.1. Develop security technical configuration and implementation validation requirements and associated expected results for IT products and services and provide automated validation capabilities to the DoD Components for use in the DIACAP.

5.3.2. Develop and provide DIACAP training and awareness products and a distributive training capability to support the DoD Components according to Reference (b) and DoDD 8570.1 (Reference (k)) and post the training materials on the IA Support Environment Web site (<http://iase.disa.mil/>).

5.3.3. Appoint a flag-level representative to the DISN/GIG Flag Panel (previously the DISN Flag Panel).

5.4. The Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) shall:

5.4.1. Appoint a PAA for DoD ISs governed by the Business MA (BMA).

5.4.2. Participate in the DIACAP TAG to ensure that the DIACAP and execution of the responsibilities established in DoDI 5000.2 (Reference (l)) are mutually supportive.

5.5. The Under Secretary of Defense for Intelligence (USD(I)) shall appoint a PAA for all DoD ISs governed by the Defense Intelligence MA (DIMA).

5.6. The Director, Defense Intelligence Agency, under the authority, direction, and control of the USD(I), shall appoint a flag-level representative to the DISN/GIG Flag Panel.

5.7. The Director, National Security Agency, under the authority, direction, and control of the USD(I), shall:

5.7.1. Develop the IA component of the GIG architecture (Reference (c)) and publish supporting implementation material in the DIACAP KS.

5.7.2. Engage the GIG IA capability, services provider, and user communities -- to include commercial, defense, and other government agencies -- to foster development and evaluation of IA implementation and validation solutions that support the DIACAP.

5.7.3. Ensure that IA security engineering services provided to the DoD Components support the DIACAP.

5.7.4. Appoint a flag-level representative to the DISN/GIG Flag Panel.

5.8. The Heads of the DoD Components shall:

5.8.1. Ensure DoD ISs under their purview comply with the DIACAP.

5.8.2. Operate only accredited ISs (i.e., those with a current ATO, interim authorization to operate (IATO), or interim authorization to test (IATT)).

5.8.3. Comply with all accreditation decisions, including denial of authorization to operate (DATO), and enforce authorization termination dates (ATD).

5.8.4. Ensure that an annual assessment of the DoD Component IA program is conducted as required by Reference (a).

5.8.5. Appoint DAAs for DoD ISs under their purview.

5.8.6. Provide training and ensure appropriate professional certification for personnel engaged in or supporting the DIACAP is consistent with Reference (k) and supporting issuances.

5.8.7. Ensure that the information owner(s) appoints a user representative(s) (UR) for DoD ISs under the DoD Component's purview.

5.8.8. In the absence of a DoD Component CIO, appoint the SIAO.

5.9. The Chairman of the Joint Chiefs of Staff shall:

5.9.1. Appoint a PAA for DoD ISs governed by the Warfighting MA (WMA).

5.9.2. Ensure that Joint Capabilities Integration and Development System (JCIDS) implementation guidance requires DIACAP planning consistent with this Instruction.

5.10. The Commander, United States Strategic Command, shall:

5.10.1. Assign DAAs for space systems used by the Department of Defense in accordance with DoDD 8581.1 (Reference (m)).

5.10.2. Accredit IS processing, storing, or transmitting Nuclear Command and Control Extremely Sensitive Information (NC2-ESI) data.

5.10.3. Appoint a flag-level representative to the DISN/GIG Flag Panel.

5.11. The PAAs shall:

5.11.1. Represent the interests of the MA and, as required, issue accreditation guidance specific to the MA, consistent with this Instruction.

5.11.2. Appoint flag-level (e.g., general officer, senior executive) PAA Representatives to the DISN/GIG Flag Panel.

5.11.3. Resolve accreditation issues within their respective MAs and work with other PAAs to resolve issues among MAs, as needed.

5.11.4. Designate DAAs for MA ISs, if required, in coordination with appropriate DoD Components.

5.12. The PAA Representatives shall:

5.12.1. Serve as members of the DISN/GIG Flag Panel.

5.12.2. Provide MA-related guidance to DAAs, Milestone Decision Authorities (Reference (j)), the DSAWG, and the DIACAP TAG.

5.12.3. Advise the corresponding MA PAAs and assist the ASD(NII)/DoD CIO and SIAO in assessing the effectiveness of GIG IA capabilities.

5.13. The DoD Component CIOs shall:

5.13.1. Appoint a DoD Component SIAO in accordance with Reference (a) to direct and coordinate the DoD Component IA program consistent with the strategy and direction of the Defense-wide Information Assurance Program (DIAP).

5.13.2. Ensure that implementation and validation of IA controls through the DIACAP are incorporated as an element of the DoD Component IS life-cycle management processes.

5.13.3. Ensure that the C&A status of the DoD Component ISs is visible to the ASD(NII)/DoD CIO and PAAs.

5.13.4. Ensure collaboration and cooperation between the DoD Component IA program and the PAA and DAA structure.

5.13.5. Verify that a program or system manager is identified for each DoD Component IS.

5.13.6. Establish and manage an IT Security POA&M program.

5.14. The DoD Component SIAOs, under the authority, direction, and control of the DoD Component CIOs, shall:

5.14.1. Establish and enforce the C&A process within the DoD Component IA program.

5.14.2. Ensure DoD Component-level participation in the DIACAP TAG.

5.14.3. Track the C&A status of ISs that are governed by the DoD Component IA program.

5.14.4. Establish and manage a coordinated IA certification process for ISs governed by the DoD Component IA program. This includes but is not limited to:

5.14.4.1. Functioning as the certifying authority (CA) or formally delegating CA for governed ISs.

5.14.4.2. Ensuring and overseeing a qualified certification cadre (e.g., validators, analysts, CA representatives).

5.14.4.3. Identifying and recommending changes and improvements to certification and validation procedures to the TAG for inclusion in the DIACAP KS.

5.14.4.4. Ensuring that DoD Component certification guidance is posted to the DoD Component portion of the KS.

5.14.5. Serve as the single IA coordination point for joint or Defense-wide programs that are deploying ISs to DoD Component enclaves.

5.15. The DAAs, in addition to the responsibilities established in Reference (d), shall:

5.15.1. Comply with DISN/GIG Flag Panel direction issued on behalf of the GIG MA PAAs.

5.15.2. Ensure a DIACAP package is initiated and completed for assigned ISs.

5.15.3. Ensure assigned DoD ISs comply with applicable DoD baseline IA controls.

5.15.4. Ensure security classification guides are established according to DoD 5200.1-R (Reference (n)).

5.15.5. Authorize or deny operation or testing of assigned DoD ISs. Coordinate with the Director, Operational Test and Evaluation before denying IATT.

5.16. The Program Manager (PM) or System Manager (SM) for DoD ISs shall:

5.16.1. Ensure that each assigned DoD IS has a designated IA manager (IAM) with the support, authority, and resources to satisfy the responsibilities established in Reference (d) and this Instruction.

5.16.2. Implement the DIACAP for assigned DoD ISs.

5.16.3. Plan and budget for IA controls implementation, validation, and sustainment throughout the system life cycle, including timely and effective configuration and vulnerability management.

5.16.4. Ensure that information system security engineering is employed to implement or modify the IA component of the system architecture in compliance with the IA component of the GIG Architecture (Reference (c)) and to make maximum use of enterprise IA capabilities and services.

5.16.5. Enforce DAA accreditation decisions for hosted or interconnected DoD ISs.

5.16.6. Develop, track, resolve, and maintain the DIACAP Implementation Plan (DIP) for assigned DoD ISs.

5.16.7. Ensure IT Security POA&M development, tracking, and resolution.

5.16.8. Ensure annual reviews of assigned ISs required by FISMA are conducted.

5.17. The DoD IS URs shall:

5.17.1. Represent the operational interests of the user community in the DIACAP.

5.17.2. Support the IA controls assignment and validation process to ensure user community needs are met.

5.18. The IAMs, in addition to the responsibilities established in Reference (d), shall:

5.18.1. Support the PM or SM in implementing the DIACAP.

5.18.2. Advise and inform the governing DoD Component IA program on DoD ISs C&A status and issues.

5.18.3. Comply with the governing DoD Component IA program information and process requirements.

5.18.4. Provide direction to the IA Officer (IAO) in accordance with Reference (d).

5.18.5. Coordinate with the organization's Security Manager to ensure issues affecting the organization's overall security are addressed appropriately.

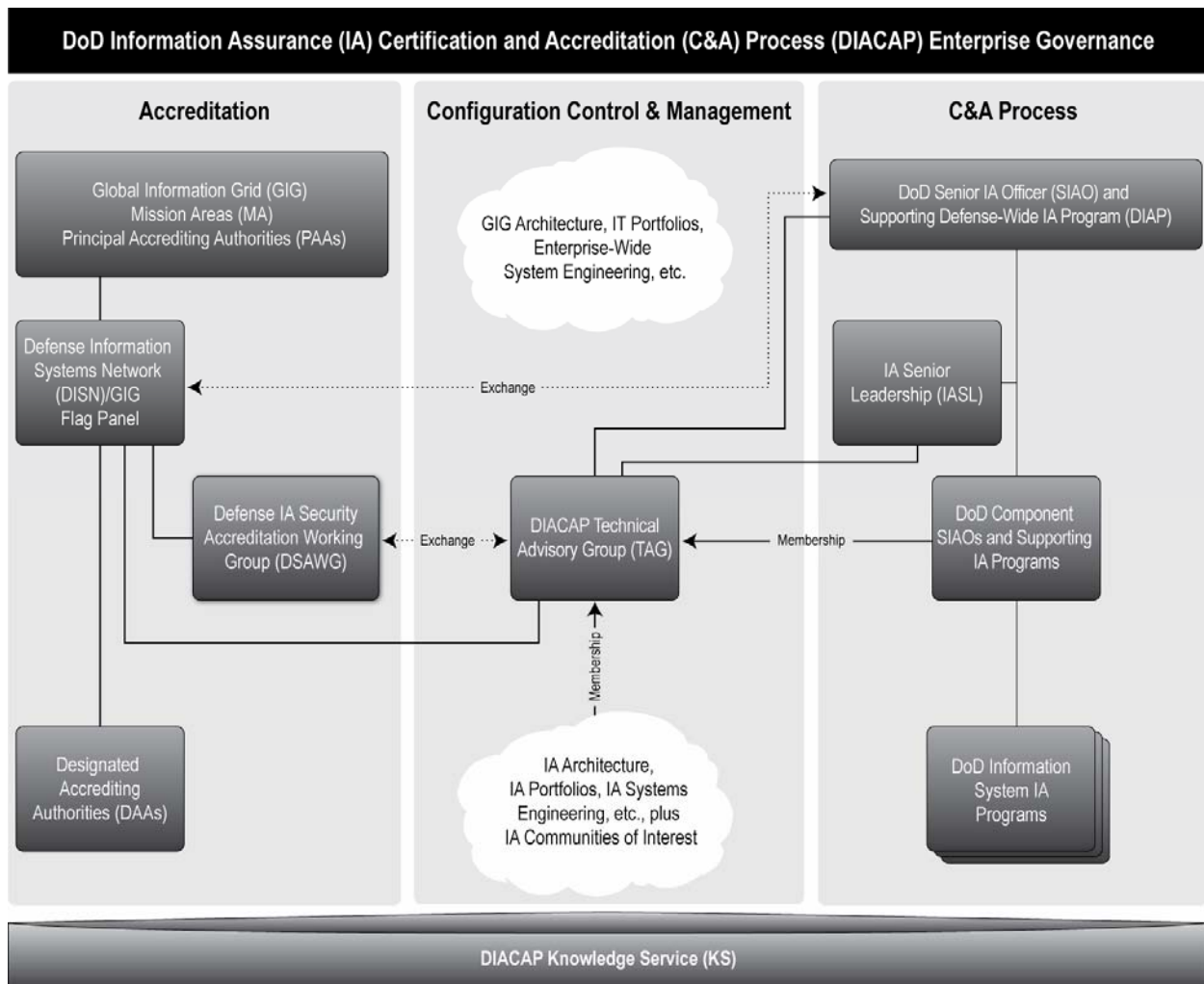
## 6. PROCEDURES

6.1. Background. This section describes the DoD procedures for identifying, implementing, validating, certifying, and managing IA capabilities and services, expressed as IA controls, and authorizing the operation of DoD ISs. It also describes the processes for configuration management of DoD IA controls and supporting implementation materials. DIACAP activities and roles are distributed across all levels of the DoD and GIG governance structures, as well as all stages of the life cycle of both the IA Component of the GIG (Reference (c)) and of individual ISs. DIACAP implementation is supported by the DIACAP KS, a Web-based DoD resource that provides the most current requirements, guidance, and tools for implementing and executing the DIACAP, including IA control implementation procedures. Enclosure 4 provides additional information on the KS.



6.2. DIACAP Enterprise Governance. This structure is intended to synchronize and integrate DIACAP activities across all levels of the DoD and GIG MAs, all aspects of the IT life cycle, and logical and organizational entities. It comprises three major elements: an accreditation structure; a CCM structure; and a C&A process structure. These elements are illustrated in Figure F1. and described in subparagraphs 6.2.1. through 6.2.4.

Figure F1. DIACAP Enterprise Governance



### 6.2.1. Accreditation

6.2.1.1. PAAs are appointed for each of the GIG MAs (i.e., the EIEMA, BMA, WMA, and DIMA). PAAs may directly appoint DAAs for DoD ISs supporting an MA Community of Interest (COI) (DoD 8320.2-G (Reference (o))). DAAs have the authority and responsibility for accreditation decisions.

6.2.1.2. The DISN/GIG Flag Panel (charter under development), acting on behalf and in support of the PAAs, is responsible for advising PAAs; assessing enterprise risk; authorizing information exchanges and connections for enterprise IS, cross-MA IS, cross security domain connections, and non-DoD connections; and approving changes to the DoD IA control baseline.

6.2.1.3. The DSAWG (DoD CIO memorandum (Reference (p))), under the DISN/GIG Flag Panel, is the community forum for reviewing and resolving C&A decisions related to the sharing of community risk. The DSAWG develops and provides guidance to the DAAs for IS connections to the GIG.

#### 6.2.2. CCM

6.2.2.1. The DIACAP TAG (ASD(NII) memorandum (Reference (q))) provides CCM of the DIACAP through interfacing with the DoD Component IA programs, IA COIs, and other entities (e.g., the GIG IA Program Office, DSAWG) to address issues that are common across all entities, by:

6.2.2.1.1. Providing detailed analysis and authoring support for the enterprise portion of the DIACAP KS content.

6.2.2.1.2. Recommending changes to the baseline IA controls to the DISN/GIG Flag Panel.

6.2.2.1.3. Recommending changes to the C&A process to the DoD SIAO.

6.2.2.1.4. Advising the IASL and other IA advisory forums identified by the DoD SIAO to resolve C&A priorities and cross-cutting issues.

6.2.2.1.5. Developing and managing DoD enterprise-level C&A automation requirements.

6.2.2.2. The TAG is supported by the DIACAP KS, described in Enclosure 4. The DIACAP KS enables TAG functions and activities, including maintenance of membership; voting, analysis, and authoring; and configuration control of KS enterprise content and functionality.

6.2.3. C&A Responsibilities. The DoD SIAO directs and coordinates the DoD IA Program. DoD Component SIAOs have authority and responsibility for certification. Each DoD Component SIAO serves as the CA for all DoD ISs assigned to or governed by the DoD Component CIO and supporting IA program. Each CA may task, organize, staff, and centralize or delegate certifying activities. Regardless of the adopted model, the SIAO is responsible for certification quality, capacity, visibility, and effectiveness. In addition, each CIO, supported by an appointed SIAO, is responsible for administration of the overall C&A process. This includes the integration of certification with other DIACAP activities, participation in the DIACAP CCM, visibility and sharing of the C&A status of assigned ISs, enforcement of training requirements

for persons participating in the DIACAP, support to DAAs, and responsiveness to the DoD CIO. The IASL (DoD CIO memorandum (Reference (r))) serves as an SIAO community forum for assessing and improving C&A process administration. The IASL provides strategic direction and guidance to ensure integrated Defense-wide IA. It provides for the integrated planning, coordination, and oversight of the Department's IA programs.

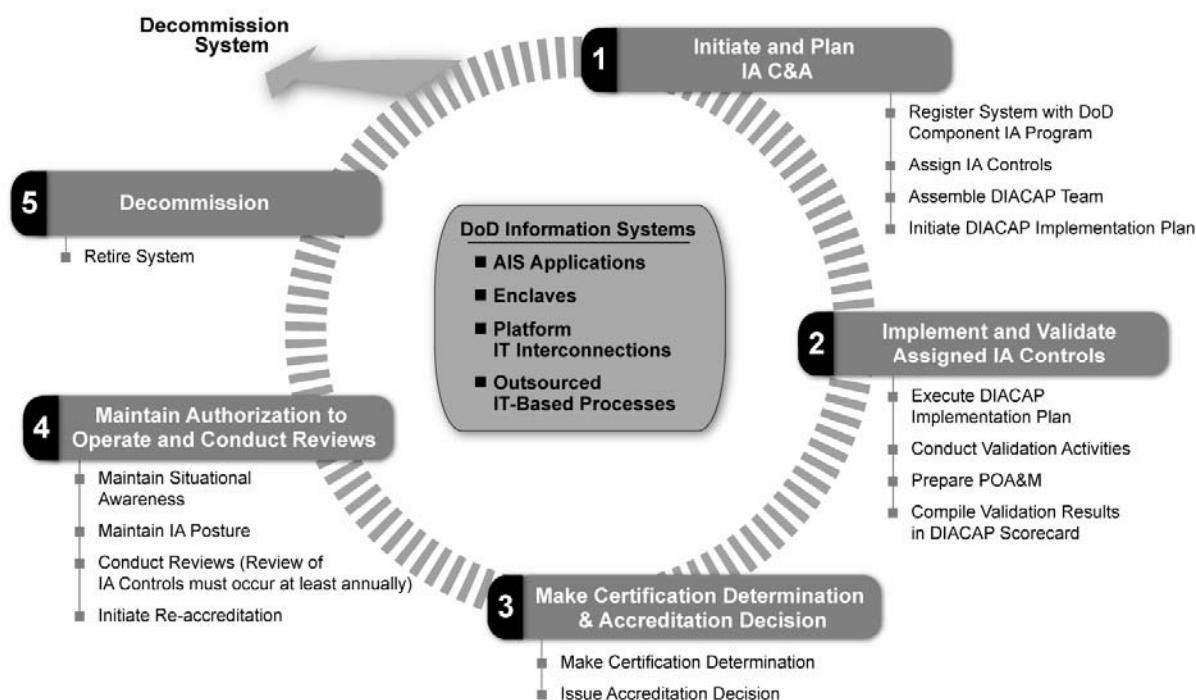
6.2.4. C&A Role Appointment. Table T1. identifies the appropriate authority for the appointment of C&A roles.

Table T1. Appointment of C&A Roles

<b>C&amp;A Role</b>	<b>Appointed By</b>
PAA	GIG MA Owner
PAA Representative	PAA
DAA	DoD Component Head or designee; PAA for MA-managed ISs
CIO	DoD Component Head
SIAO	DoD Component CIO or, in organizations in which the position of DoD Component CIO does not exist, the DoD Component Head Note: DoD SIAO appointed by DoD CIO
CA	SIAO is the Component CA, but may formally delegate the CA role as appropriate
CA Representative, Analyst, Validator	Component CA or CA delegates
IAM	PM or SM
IAO	IAM
UR	Information Owner
DIACAP TAG Representative	DoD Component SIAO or DoD Component CIO

6.3. DIACAP Activities. The DIACAP consists of the activities and tasks depicted in Figure F2. The DIACAP parallels the system life cycle, and its activities should be initiated at inception (e.g., documented during capabilities identification or at the implementation of a major system modification). However, failure to initiate the DIACAP at system inception is not a justification for ignoring or not complying with the DIACAP. Unaccredited systems shall initiate the DIACAP immediately, regardless of the system life-cycle stage (e.g., acquisition, operation).

Figure F2. DIACAP Activities



6.3.1. Initiate and Plan IA C&A. This activity includes registering the system with the governing DoD Component IA program, assigning IA controls based on Mission Assurance Category (MAC) and Confidentiality Level (CL), identifying the DIACAP Team for the IS, and initiating the IS's DIP.

6.3.1.1. Register the System with the DoD IA Program. System registration establishes the relationship between the DoD IS and the governing DoD Component IA program which continues until the DoD IS is decommissioned. DIACAP registration is related to other DoD initiatives to collect IT-related information (e.g., the Defense Information Technology Portfolio Repository); however, specific registration instructions change over time and are therefore maintained through the DIACAP CCM and published in the DIACAP KS. The System Identification Profile (SIP) is generated during the registration process and becomes part of the DIACAP package for the IS. Attachment 1 to Enclosure 3 of this Instruction identifies the minimum data requirements and explanations for the SIP.

6.3.1.2. Assign IA Controls. Identifying applicable IA controls for an information system is a critical activity in the DIACAP. There are four basic steps in assigning the IA controls: determining the type of information system; determining the MAC and CL for the information system; identifying the baseline IA controls; and augmenting the baseline IA controls.

6.3.1.2.1. Baseline IA controls originate from Reference (d) control sets, are based on MAC and CL, and are implemented through procedures presented in the DIACAP KS.

6.3.1.2.2. Baseline IA control sets can be augmented with additional IA controls to address special security needs or unique requirements of the IS(s) to which they apply. Augmenting IA controls originate from an MA, a DoD Component, a COI, or a local system. Augmenting IA controls must neither contradict nor negate DoD baseline IA controls, must not degrade interoperability across the DoD Enterprise, and may not be used as a basis for denying connectivity of systems that have met the DoDI 8500.2 baseline IA controls for MAC and CLs of the gaining IS. Procedures for implementing augmenting IA controls are the responsibility of the originator.

6.3.1.2.3. Assigned IA controls may be inherited. Inheritance refers to situations where IA controls along with their validation results and compliance status are shared by two or more systems for the purposes of C&A. Through inheritance, an existing IA control and its compliance status extends from an originating IS to a receiving IS. Inheritance eliminates the need for the receiving systems to duplicate testing and documentation of inherited IA controls. The DIP specifically identifies IA controls inherited from other systems. The compliance status of IA controls inherited from the originating IS is reflected on the DIACAP Scorecard of the receiving IS.

6.3.1.3. Assemble the DIACAP Team

6.3.1.3.1. The members of the DIACAP Team are required to meet the trustworthiness investigative levels for users with IA management access to DoD unclassified ISs as established in Section E3.4.8. of Reference (d). SIAOs shall meet the same investigative requirements as those for DAA, and certification cadre members shall meet the same requirements as those established for monitoring and testing in Table E3.T1. of Reference (d).

6.3.1.3.2. DIACAP Team members will be trained and certified in accordance with Reference (k), as required.

6.3.1.3.3. Allowable relationships among DIACAP Team members are outlined in Table T2.

Table T2. Allowable Relationships Among DIACAP Team Members

<b>Relationships</b>	<b>Allowed (Y/N)</b>
PAA may be a DAA	Yes
DAA reports to the PM, SM, or Program Executive Officer (PEO)	No
DAA and CA for a DoD IS may be the same person	Yes
CIO may be a DAA	Yes
CA reports to a DAA	Yes
CA reports to the PM , SM, or PEO	No
PM or SM and CA both report to the DAA	Yes
PM or SM and CA for a DoD IS may be the same person	No
PM or SM and DAA for a DoD IS may be the same person	No
PM or SM and UR for a DoD IS may be the same person	No
PM or SM reports to CA	No
PM or SM reports to the CIO	Yes
PM or SM reports to the DAA	Yes
UR reports to the CIO	Yes
UR reports to the PM or SM	No
UR reports to the SIAO/CA	Yes

6.3.1.4. Initiate the DIP. This plan contains the IS's assigned IA controls, including inherited IA controls. The plan also includes the IA control implementation status, responsible entities, resources, and the estimated completion date for each assigned IA control. The plan may reference applicable supporting implementation material and artifacts.

6.3.2. Implement and Validate Assigned IA Controls. This activity includes executing the DIP, conducting validation activities, preparing the IT Security POA&M, and compiling the validation results in the DIACAP Scorecard.

6.3.2.1. Execute the DIP. Each assigned IA control is implemented according to the applicable implementation guidelines described in the DIACAP KS.

6.3.2.2. Conduct Validation Activities. Validation procedures are maintained through the DIACAP CCM and published in the DIACAP KS. Each validation procedure describes requisite preparatory steps and conditions, actual validation steps, expected results, and criteria and protocols for recording actual results. Each procedure includes associated supporting background material, sample results, or links to automated testing tools. Actual results are recorded according to the criteria and protocols specified in the validation procedure and are made a permanent part of the comprehensive DIACAP package, along with any artifacts produced during the validation (e.g., output from automated test tools or screen shots that depict aspects of system configuration). For inherited IA controls, validation test results and supporting documentation are maintained by the originating IS and are made available to CAs of receiving ISs on request.

6.3.2.3. Record Compliance Status. The status of each assigned IA control is indicated on the DIACAP Scorecard. An example of a Scorecard and discussion of its fields are provided in Attachment 2 to Enclosure 3.

6.3.2.3.1. Compliant (C) IA controls are those for which the expected results for all associated validation procedures have been achieved.

6.3.2.3.2. Non-compliant (NC) IA controls are those for which one or more of the expected results for all associated validation procedures are not achieved. Not achieving expected results for all validation procedures does not necessarily equate to unacceptable risk.

6.3.2.3.3. Not applicable (NA) IA controls are those that do not impact the IA posture of the IS as determined by the DAA.

6.3.2.4. Prepare an IT Security POA&M. An IT Security POA&M identifies tasks that need to be accomplished. It specifies resources required to accomplish the elements of the plan and milestones for completing tasks, along with their scheduled completion dates. IT Security POA&Ms are permanent records. Once posted, weaknesses will be updated, but not removed, after correction or mitigation actions are completed. Inherited weaknesses are reflected on the IT Security POA&Ms. IT Security POA&Ms may be active or inactive throughout a system's life cycle as weaknesses are newly identified or closed. The DoD Component CIOs are responsible for monitoring and tracking the overall execution of system-level IT Security POA&Ms until identified security weaknesses have been closed and the C&A documentation appropriately adjusted. The DAAs are responsible for monitoring and tracking overall execution of system-level IT Security POA&Ms. The PM or SM is responsible for implementing the corrective actions identified in the IT Security POA&M and, with the support and assistance of the IAM, provides visibility and status to the DAA, the SIAO, and the

governing DoD Component CIO. In order to reflect the complete IA posture of a DoD IS at all times in a single document, the IT Security POA&M is also used to document DAA-accepted NC IA controls and baseline IA controls that are NA because of the nature of the system. A full discussion and templates for preparing an IT Security POA&M are provided in Attachment 3 to Enclosure 3.

### 6.3.3. Make Certification Determination and Accreditation Decision

#### 6.3.3.1. The CA makes certification determinations.

6.3.3.1.1. A CA representative is an active member of the DIACAP Team from inception and continuously assesses and guides the quality and completeness of DIACAP activities and tasks and the resulting artifacts.

#### 6.3.3.1.2. Certification considers:

6.3.3.1.2.1. The overall reliability and viability of the DoD IS plus the acceptability of the implementation and performance of IA mechanisms or safeguards inherent in the system.

6.3.3.1.2.2. The system behavior in the larger information environment, including consideration of vulnerabilities to the environment, correct and secure interactions with the information environment management and control services, and visibility into situational awareness and network defense services.

6.3.3.1.3. Impact codes are assigned by the TAG to IA controls at the time of authoring and are maintained through the DIACAP CCM. They indicate the TAG's assessment of the consequences of a failed IA control. Impact codes are expressed as high, medium, and low, with high indicating the greatest impact. In conjunction with the severity category, the impact code indicates the urgency with which corrective action should be taken. Within a severity category, non-compliant IA controls should be prioritized for correction or remediation according to their impact codes.

6.3.3.1.4. Severity categories are assigned to a system weakness or shortcoming by a CA or a designated representative as part of a certification analysis to indicate the risk level associated with the security weakness and the urgency with which the corrective action must be completed. Severity categories are expressed as category (CAT) I, CAT II, and CAT III. Severity categories are assigned after considering all possible mitigation measures that have been implemented within system design and architecture limitations for the DoD IS in question. For instance, what may be a CAT I weakness in a component part of a system (e.g., a workstation or server) may be offset or mitigated by other protections within hosting enclaves so that the overall risk to the system is reduced to a CAT II.



6.3.3.1.4.1. CAT I weaknesses shall be corrected before an ATO is granted.

6.3.3.1.4.2. CAT II weaknesses shall be corrected or satisfactorily mitigated before an ATO can be granted.

6.3.3.1.4.3. CAT III weaknesses will not prevent an ATO from being granted if the DAA accepts the risk associated with the weaknesses.

6.3.3.1.5. The certification determination is based on the actual validation results. It considers impact codes associated with IA controls in a non-compliant status, associated severity categories, expected exposure time (i.e., the projected life of the system release or configuration minus the time to correct or mitigate the IA security weakness), and cost to correct or mitigate (e.g., dollars, functionality reductions). The weaknesses identified on the IT Security POA&M reflect residual risk to the system. See Attachment 3 to Enclosure 3 for further discussion on IT Security POA&M formulation.

6.3.3.1.6. A certification determination is always required before an accreditation decision. If a compelling mission or business need requires the rapid introduction of a new DoD IS into the GIG, validation activity and a certification determination are still required. If the operation will be required beyond the time period of an IATO, a complete validation should be initiated immediately.

6.3.3.2. The DAA issues accreditation decisions.

6.3.3.2.1. An accreditation decision is communicated via the DIACAP Scorecard and accompanying IT Security POA&M, if required.

6.3.3.2.2. Documentation (e.g., artifacts, actual validation results) supporting an accreditation decision will be provided in electronic form if requested by DAAs of interconnecting systems.

6.3.3.2.3. An accreditation decision always applies to a specifically identified DoD IS and is based on a balance of mission or business need, protection of personal privacy, protection of the information being processed, and protection of the information environment and thus, by extension, protection of other missions or business functions reliant on the shared information environment.

6.3.3.2.4. An accreditation decision always requires a certification determination. If the validation is abbreviated as a result of mission urgency, the accreditation decision cannot exceed an IATO. If operation will be required beyond the time period of an IATO, a complete validation should be initiated immediately.

6.3.3.2.5. When there is compelling operational necessity, DoD ISs may be allowed to operate despite IT security weaknesses that cannot be corrected or adequately mitigated within prescribed timeframes because of technology limitations or, in rare cases, prohibitive costs. Such instances must be fully justified, approved, and documented.

6.3.3.2.6. An accreditation decision is expressed as an ATO, an IATO, an IATT, or a DATO. A system is considered unaccredited if an accreditation decision has not been made.

6.3.3.2.6.1. ATO

6.3.3.2.6.1.1. An ATO accreditation decision must specify an authorization termination date that is within 3 years of the authorization date.

6.3.3.2.6.1.2. A system with a CAT I weakness may not be granted an ATO. A system can operate with a CAT I weakness only when it is critical to military operations as determined by affected military commanders and if failure to deploy or allow continued operation for deployed systems will preclude mission accomplishment. When requested by an affected military commander, the DoD Component CIO shall authorize operation of a system with a CAT I weakness through an IATO. This responsibility cannot be delegated below the DoD Component CIO, and a signed copy of the authorization memorandum with supporting rationale shall be provided to the DoD SIAO and the system's DAA.

6.3.3.2.6.1.3. A system with a CAT II weakness can be granted an ATO only when there is clear evidence that the CAT II weakness can be corrected or satisfactorily mitigated within 180 days of the accreditation decision.

6.3.3.2.6.1.4. An ATO can be granted with CAT III weaknesses. The DAA will determine if these weaknesses will be corrected or the risk accepted. CAT III weaknesses accepted by the DAA will appear on the IT Security POA&M with the "Resources Required," "Scheduled Completion Date," "Milestones with Completion Dates," and "Milestone Changes" columns marked "NA," and with the "Status" column marked "Risk Accepted by DAA."

6.3.3.2.6.2. IATO

6.3.3.2.6.2.1. An IATO accreditation decision is intended to manage IA security weaknesses while allowing system operation. It is not intended to be a device for signaling an evolutionary acquisition. A version of a DoD IS acquired in one of a planned series of acquisition increments or development spirals should be granted an ATO, even if additional or enhanced capabilities and services are planned for future increments or spirals. The ATO accreditation decision should not be reserved for DoD ISs for which no change is planned or foreseen. Such thinking engenders an abuse of the IATO accreditation status and is an inaccurate portrayal of the DoD ISs' IA posture.

6.3.3.2.6.2.2. An IATO accreditation decision must specify an ATD that is within 180 days of the authorization date. A DAA may not grant consecutive IATOs totaling more than 360 days.

6.3.3.2.6.2.3. A request for an IATO must be accompanied by an IT Security POA&M that documents identified weaknesses and specifies corrective measures, as appropriate. Corrective actions specified in the IT Security POA&M must be achievable within the authorization period and resourced accordingly.

6.3.3.2.6.2.4. If CAT II weaknesses have not been corrected or satisfactorily mitigated after system operation under IATOs for a total of 360 days, the DAA will normally issue a DATO that will remain in effect until all corrective actions identified in the IT Security POA&M are implemented satisfactorily and the DAA is able to grant an ATO.

6.3.3.2.6.2.5. The DoD Component CIO may authorize continuation of operation under IATO for systems with CAT II weaknesses that have operated for 360 consecutive days. This responsibility cannot be delegated below the DoD Component CIO. The DAA must certify in writing or through DoD PKI-certified digital signature that continued system operation is critical to mission accomplishment. A copy of the authorization to continue system operation with supporting rationale shall be provided to the DoD SIAO.

#### 6.3.3.2.6.3. IATT

6.3.3.2.6.3.1. The IATT accreditation decision is a special case for authorizing testing in an operational information environment or with live data for a specified time period. IATTs should be granted only when operational environment/live data is required to complete specific test objectives (e.g., replicating certain operating conditions in the test environment is impractical).

6.3.3.2.6.3.2. All applicable IA controls should be tested and satisfied prior to testing in an operational environment or with live data except for those which can only be tested in an operational environment. In consultation with the PM or SM, the DAA will determine which IA controls can only be tested in an operational environment.

6.3.3.2.6.3.3. An IATT may not be used to avoid ATO or IATO validation activity and certification determination requirements for authorizing a system to operate. Operation of a system under an IATT in an operational environment is for testing purposes only (i.e., the system will not be used for operational purposes during the IATT period).

6.3.3.2.6.4. DATO. A DATO will be issued if the DAA determines that a DoD IS should not operate because the IA design is inadequate, assigned IA controls are not adequately implemented, or because of a lack of other adequate security is revealed through certification activities and there are no compelling reasons to allow system operation under subparagraphs 6.3.3.2.6.1.2 or 6.3.3.2.6.2.5. If the system is already operational, the DAA will issue a DATO and halt operation of the system immediately.

6.3.4. Maintain Authorization to Operate and Conduct Reviews. Continued ATO is contingent on the sustainment of an acceptable IA posture. The DoD IS IAM has primary responsibility for maintaining situational awareness and initiating actions to improve or restore IA posture.

6.3.4.1. Maintain Situational Awareness. Included in the IA controls assigned to all DoD ISs are IA controls related to configuration and vulnerability management, performance monitoring, and periodic independent evaluations (e.g., penetration testing). The IAM continuously monitors the system or information environment for security-relevant events and configuration changes that negatively impact IA posture and periodically assesses the quality of IA controls implementation against performance indicators such as security incidents, feedback from external inspection agencies (e.g., IG DoD, Government Accountability Office (GAO)), exercises, and operational evaluations. In addition the IAM may, independently or at the direction of the CA or DAA, schedule a revalidation of any or all IA controls at any time. Reference (a) requires revalidation of a select number of IA controls at least annually.

6.3.4.1.1. DoD ISs with a current ATO that are found to be operating in an unacceptable IA posture through GAO audits, IG DoD audits, or other reviews or events such as an annual security review or compliance validation shall have the newly identified weakness added to an existing or newly created IT Security POA&M.

6.3.4.1.2. If a newly discovered CAT I weakness on a DoD IS operating with an ATO cannot be corrected within 30 days, the system can only continue operation under the terms prescribed in subparagraph 6.3.3.2.6.1.2.

6.3.4.1.3. If a newly discovered CAT II weakness on a DoD IS operating with a current ATO cannot be corrected or satisfactorily mitigated within 90 days, the system can only continue operation under the terms prescribed in subparagraph 6.3.3.2.6.2.5.

6.3.4.2. Maintain IA Posture. The IAM may recommend changes or improvement to the implementation of assigned IA controls, the assignment of additional IA controls, or changes or improvements to the design of the IS itself.

6.3.4.3. Perform Reviews. The IAM shall annually provide a written or DoD PKI-certified digitally signed statement to the DAA and the CA that indicates the results of the security review of all IA controls and the testing of selected IA controls as required by Reference (a). The review will either confirm the effectiveness of assigned IA controls and their implementation, or it will recommend: changes such as those described in subparagraph 6.3.4.2.; a change in accreditation status (e.g., accreditation status is downgraded to IATO or DATO); or development of an IT Security POA&M. The CA and DAA shall review the IAM statement in light of mission and information environment indicators and determine a course of action that will be provided to the concerned CIO or SIAO for reporting requirements described in Reference (a). The date of the annual security review will be recorded in the SIP. A DAA may downgrade or revoke an accreditation decision at any time if risk conditions or concerns so warrant.

6.3.4.4. Initiate Reaccreditation. In accordance with OMB Circular A-130 (Reference (s)), an IS must be recertified and reaccredited once every 3 years. The results of an annual review or a major change in the IA posture at any time may also indicate the need for recertification and reaccreditation of the IS.

6.3.5. Decommission. When a DoD IS is removed from operation, a number of DIACAP-related actions are required. Prior to decommissioning, any inheritance relationships should be reviewed and assessed for impact. Once the system has been decommissioned, Lines 8, “DIACAP Activity,” and 9, “System Life Cycle Phase,” of the SIP should be updated to reflect the IS decommissioned status. Concurrently, the DIACAP Scorecard and any POA&Ms should also be removed from all tracking systems. Other artifacts and supporting documentation should be disposed of according to its sensitivity or classification. Data or objects in IA infrastructures that support the GIG, such as key management, identity management, vulnerability management, and privilege management, should be reviewed for impact.

6.4. Transition to DIACAP. All DoD ISs are required to transition to the DIACAP in accordance with the timeline and instructions specified in Enclosure 5. The DoD Components are responsible for ensuring that all assigned DoD ISs meet the specified timelines.

6.5. IA Product Evaluation and DIACAP Evaluation. The DIACAP validation of a DoD IS that consists of a single IA -enabled product or solution (e.g., an IA-enabled database management system) may also serve as the IA-enabled product evaluation. These conditions are reiterated in Table T3.

Table T3. IA Product Evaluation and DIACAP Evaluation

Condition	Acceptable Evaluation/Validation Approach
Accreditation boundary includes both IT products or services and IA or IA-enabled IT products.	<ol style="list-style-type: none"> <li>1. National Security Telecommunications and ISs Security Policy No.11 (Reference (t)) evaluation for IA and IA-enabled products; and</li> <li>2. DIACAP for overall system design and configuration.</li> </ol>
Proposed accreditation boundary includes ONLY a single IT product or service that is IA-enabled and nothing else.	DIACAP validation is sufficient; separate Reference (t) evaluation is not required.

6.6. System Interconnection. Reference (s) requires “written management authorization, based upon the acceptance of risk to the system, prior to connecting with other systems.” DoD ISs generally satisfy this requirement through compliance with connection management procedures established by the Chairman of the Joint Chiefs of Staff. Separately accredited ISs that communicate directly through tightly coupled mechanisms, such as shared memory or direct code invocation, are not subject to this requirement. In addition, for IA purposes, loosely coupled ISs (e.g., by proxy) communicating via Web services are not considered system interconnections and do not require connection approval, a security memorandum, or written management authorization. Dynamic interaction among accredited software systems that have been designed to interact is not considered a security-relevant event. This includes authorized messaging with non-DoD ISs (e.g., electronic commerce/electronic data interchange transactions with an IS belonging to another department or agency).

6.7. Type Accreditation. The type accreditation is the official authorization to employ identical copies of a system in specified environments. This form of C&A allows a single DIACAP package (i.e., SIP, DIP, supporting documentation for certification, DIACAP Scorecard, and IT Security POA&M (if required)) to be developed for an archetype (common) version of an IS that is deployed to multiple locations, along with a set of installation and configuration requirements or operational security needs, that will be assumed by the hosting location. Automated Information System (AIS) applications accreditations are type accreditations. Stand-alone IS and demilitarized zone (DMZ) accreditations may also be type accreditations.

6.8. Stand-Alone IS Accreditation. Stand-alone ISs are treated as special types of enclaves that are not interconnected to any other network. Stand-alone systems do not transmit, receive, route, or interchange information outside of the system’s accreditation boundary. IA requirements for a stand-alone system are determined by its MAC and classification or sensitivity and need-to-know just as for other DoD ISs. Stand-alone systems must always be clearly identified as such on the IT Security POA&M, the SIP, and the DIACAP Scorecard. Because of the unique architecture of a stand-alone system, certain IA controls do not pose a risk to the system as a result of their non-implementation and thus are considered NA. NA IA controls are labeled as NA on the DIACAP Scorecard and addressed on the IT Security POA&M simply as a means to document and explain why the IA control is NA in the comments column. Refer to the KS for a discussion of IA controls that may be considered NA for stand-alone systems. Additionally, stand-alone systems that are deployed to multiple locations may be type accredited.

6.9. Outsourced IT-Based Processes. Outsourced IT-based processes supported by private sector ISs, outsourced ITs, and outsourced information services fall into two sub-categories that are treated differently for C&A purposes.

6.9.1. Outsourced IT-Based Processes Established for DoD Purposes Only. Outsourced IT-based processes that are dedicated to DoD processing and are effectively under DoD configuration control (e.g., the Navy Marine Corps Intranet) are certified and accredited as DoD enclaves. Typically, outsourced IT-based processes that are MAC I are in this sub-category and those that process classified information can only be in this sub-category.

6.9.2. Outsourced IT-Based Processes That Also Support Non-DoD Users. Outsourced IT-based processes that may also support non-DoD users or processes must still be certified and accredited by DoD entities. IA requirements for DoD information in an outsourced environment are determined by its MAC and classification or sensitivity and need-to-know just as for other DoD ISs. However, the following also applies.

6.9.2.1. Technical security of the outsourced environment is the responsibility of the service provider.

6.9.2.2. Outsourced applications that are accessed by DoD users from DoD enclaves (e.g., Powertrack) are subject to DoD enclave boundary defense IA controls for incoming traffic (e.g., ports and protocols and mobile code).

6.9.2.3. Responsibility for procedural and administrative security is shared between the service provider and the supported DoD entity contracting for the service.

6.9.2.4. Security responsibilities of the service provider down to the control level are made explicit in the contract, along with any other performance and service-level parameters by which the Department of Defense shall measure the IA profile of the outsourced IT-based process for the purpose of C&A.

6.9.2.5. Any baseline IA controls that are not explicit in the contract or otherwise covered by a service level agreement are categorized as NC. All such NC IA controls must be documented in an IT Security POA&M with an explanation as to why accepting the risk of operating the outsourced IT-based process with that control in an NC status is acceptable.

6.9.2.6. Security roles and responsibilities are to be made explicit in the acquisition along with the performance and service-level parameters by which the Department of Defense shall measure the IA profile of the outsourced IT-based process. The PM for an outsourced IT-based process will need to carefully define and assess the functions to be performed and identify the technical and procedural security requirements that must be satisfied in the acquisition in order to protect DoD information in the service provider's operating environment and interconnected DoD ISs.

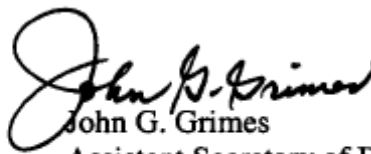
## 7. INFORMATION REQUIREMENTS

7.1. The annual assessment of the DoD Component IA programs for presentation in the annual report to Congress has been assigned Report Control Symbol (RCS) DD-NII(Q,A)2296 in accordance with DoD 8910.1-M (Reference (u)).

7.2. The DIACAP Package Contents and the review of proposed changes to the IA processes, procedures, and tools are exempt from licensing in accordance with paragraphs C4.4.2 and C4.4.3. of Reference (u).

## 8. EFFECTIVE DATE

This Instruction is effective immediately. Specific DoD IS transition timelines and instructions are provided in Enclosure 5.



John G. Grimes  
Assistant Secretary of Defense for Networks  
and Information Integration/  
DoD Chief Information Officer

### Enclosures – 5

- E1. References, continued
- E2. Definitions
- E3. The DIACAP Package
- E4. DIACAP KS Overview
- E5. DIACAP Transition Timeline and Instructions



E1. ENCLOSURE 1

REFERENCES, continued

- (e) DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997 (hereby canceled)
- (f) DoD Manual 8510.1-M, "Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual," July, 2000 (hereby canceled)
- (g) Assistant Secretary of Defense for Networks and Information Integration/ DoD Chief Information Officer Memorandum, "Interim Department of Defense (DoD) Information Assurance (IA) Certification and Accreditation (C&A) Process Guidance," July 6, 2006 (hereby canceled)
- (h) Section 11331 of title 40, United States Code
- (i) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended
- (j) DoD Directive 8115.01, "Information Technology Portfolio Management," October 10, 2005
- (k) DoD Directive 8570.1, "Information Assurance Training, Certification, and Workforce Management," August 15, 2004
- (l) DoD Instruction 5000.2, "Operation of the Defense Acquisition System," May 12, 2003
- (m) DoD Directive 8581.1, "Information Assurance (IA) Policy for Space Systems Used by the Department of Defense," June 21, 2005
- (n) DoD 5200.1-R "Information Security Program," January 1997
- (o) DoD 8320.2-G, "Guidance for Implementing Net-Centric Data Sharing," April 12, 2006
- (p) Department of Defense (DoD) Chief Information Officer (CIO) Memorandum, Charter, "DISN Security Accreditation Working Group (DSAWG)," March 26, 2004<sup>1</sup>
- (q) Assistant Secretary of Defense Networks and Information Integration Memorandum, "Charter of the Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP) Technical Advisory Group (TAG)," July 26, 2007<sup>2</sup>
- (r) Department of Defense (DoD) Chief Information Officer (CIO) Memorandum "Charter of IA Senior Leadership Group," March 5, 2004<sup>3</sup>
- (s) Appendix III to Office of Management and Budget Circular No. A-130, "Security of Federal Automated Information Resources," (Revised)
- (t) National Security Telecommunications and Information Systems Security Policy No. 11, "National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products," June 2003
- (u) DoD 8910.1-M, "Procedures for Management of Information Requirements," June 1998
- (v) Committee on National Security Systems Instruction No. 4009, "National Information Assurance (IA) Glossary," as revised June 2006
- (w) Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," as amended

---

<sup>1</sup> Available at <http://www.iase.disa.smil.mil/dsawg>

<sup>2</sup> Available at <https://diacap.iaportal.navy.mil/ks>

<sup>3</sup> Available at <https://powhatan.iiie.disa.mil/iasl-iasg/charters.html>

- (x) DoD Directive 8320.2, "Data Sharing in a Net-Centric Department of Defense," April 23, 2007
- (y) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
- (z) OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies," December 16, 2003
- (aa) OMB Memorandum, "FY 2004 Reporting Instructions for the Federal Information Security Management Act," August 23, 2004
- (ab) OMB Circular No. A-11, "Preparation, Submission, and Execution of the Budget," June 2006

## E2. ENCLOSURE 2

### DEFINITIONS

E2.1. Accreditation Boundary. See Reference (v).

E2.2. Accreditation Decision. A formal statement by a designated accrediting authority (DAA) regarding acceptance of the risk associated with operating a DoD information system (IS) and expressed as an authorization to operate (ATO), interim ATO (IATO), interim authorization to test (IATT), or denial of ATO (DATO). The accreditation decision may be issued in hard copy with a traditional signature or issued electronically signed with a DoD public key infrastructure (PKI)-certified digital signature.

E2.3. Adequate Security. See Reference (v).

E2.4. Artifacts. System policies, documentation, plans, test procedures, test results, and other evidence that express or enforce the information assurance (IA) posture of the DoD IS, make up the certification and accreditation (C&A) information, and provide evidence of compliance with the assigned IA controls.

E2.5. Assigned IA Controls. The set of IA controls that a given DoD IS must address to achieve an adequate IA posture. Consist of baseline IA controls plus any augmenting IA controls.

E2.6. Augmenting IA Controls. IA controls that augment baseline IA controls to address special security needs or unique requirements (e.g., cross security domain solutions, health information portability, privacy, etc.) of the IS(s) to which they apply. Augmenting IA controls may originate from a mission area (MA), a DoD Component, a Community of Interest (COI), or a local system. Augmenting IA controls must neither contradict nor negate DoD baseline IA controls and must not degrade interoperability across the DoD Enterprise.

E2.7. Authorization Termination Date (ATD). The date assigned by the DAA that indicates when an ATO, IATO, or IATT expires.

E2.8. Authorization to Operate (ATO). Authorization granted by a DAA for a DoD IS to process, store, or transmit information. An ATO indicates a DoD IS has adequately implemented all assigned IA controls to the point where residual risk is acceptable to the DAA. ATOs may be issued for up to 3 years.

E2.9. Baseline IA Controls. The minimum set of IA controls that must be addressed to achieve adequate security. Baseline IA controls are prescribed by DoDI 8500.2 (Reference (d)) based on mission assurance category (MAC) and confidentiality level (CL).

E2.10. Certification. For the purpose of this Instruction, a comprehensive evaluation and validation of a DoD IS to establish the degree to which it complies with assigned IA controls based on standardized procedures.

E2.11. Certification Determination. A CA's determination of the degree to which a system complies with assigned IA controls based on validation results. It identifies and assesses the residual risk with operating a system and the costs to correct or mitigate IA security weaknesses as documented in the Information Technology (IT) Security Plan of Action and Milestones (POA&M).

E2.12. Certifying Authority (CA). The senior official having the authority and responsibility for the certification of ISs governed by a DoD Component IA program.

E2.13. Certifying Authority Representative. An official appointed by and acting on behalf of the CA.

E2.14. Communities of Interest (COIs). For the purpose of this Instruction, the inclusive term used to describe groups of individuals who share information relative to common goals, interests, missions, or business processes.

E2.15. Community Risk. See Reference (b).

E2.16. Confidentiality Level (CL). See Reference (d).

E2.17. Core Enterprise Services (CESs). For the purpose of this Instruction, a set of common services intended to provide, enable, or improve access; enable information sharing; and enhance interoperability among Global Information Grid (GIG) entities. CESs enable service-oriented architectures and may include Web services. Examples of CESs include enterprise services management, messaging, discovery, mediation, collaboration, hosting, storage, IA/security, metadata services, and user assistance.

E2.18. Denial of Authorization to Operate (DATO). A DAA decision that a DoD IS cannot operate because of an inadequate IA design, failure to adequately implement assigned IA controls, or other lack of adequate security. If the system is already operational, the operation of the system is halted.

E2.19. Designated Accrediting Authority (DAA). The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with designated approving authority and delegated accrediting authority. (Reference (d) leads with the term designated approving authority, which was favored at the time of publication.)

E2.20. DIACAP Implementation Plan (DIP). Contains the IS's assigned IA controls. The plan also includes the implementation status, responsible entities, resources, and the estimated completion date for each assigned IA control. The plan may reference applicable supporting implementation material and artifacts.

E2.21. DIACAP Knowledge Service (KS). A Web-based repository of information and tools for implementing the DIACAP that is maintained through the DIACAP Technical Advisory Group (TAG).

E2.22. DIACAP Package. The collection of documents or collection of data objects generated through DIACAP implementation for an IS. A DIACAP package is developed through implementing the activities of the DIACAP and maintained throughout a system's life cycle. Information from the package is made available as needed to support an accreditation or other decision such as a connection approval. There are two types of DIACAP packages:

E2.22.1. The Comprehensive Package contains all of the information connected with the certification of the IS. It includes the System Identification Profile (SIP), the DIACAP Implementation Plan (DIP), the Supporting Certification Documentation, the DIACAP Scorecard, and the IT Security POA&M, if required.

E2.22.2. The Executive Package contains the minimum information for an accreditation decision. It contains the SIP, the DIACAP Scorecard, and the IT Security POA&M, if required.

E2.23. DIACAP Scorecard. A summary report that succinctly conveys information on the IA posture of a DoD IS in a format that can be exchanged electronically. It shows the implementation status of a DoD IS's assigned IA controls (i.e., compliant (C), non compliant (NC), or not applicable (NA)) as well as the C&A status.

E2.24. DIACAP Technical Advisory Group (TAG). A formally chartered body established by Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer to examine and address common C&A issues, including changes to the baseline IA controls, across the DoD Component IA programs, IA COIs, and other GIG entities. The DIACAP TAG also maintains configuration control and management of the DIACAP and all its supporting content on the DIACAP KS.

E2.25. DIACAP Team. Comprised of the individuals responsible for implementing the DIACAP for a specific DoD IS. At a minimum the DIACAP Team includes the DAA, the CA, the DoD IS program manager (PM) or system manager (SM), the DoD IS IA manager (IAM), IA officer (IAO), and a user representative (UR) or their representatives.

E2.26. DoD-Controlled IS. An IS that is established only for DoD purposes, dedicated to DoD processing, and is effectively under DoD configuration control (e.g., the Navy Marine Corps Intranet).

E2.27. DoD Information Assurance Certification and Accreditation Process (DIACAP). The DoD process for identifying, implementing, validating, certifying, and managing IA capabilities and services, expressed as IA controls, and authorizing the operation of DoD ISSs, including testing in a live environment, in accordance with statutory, Federal, and DoD requirements.

E2.28. DoD Information Systems. See Reference (b).

E2.29. Enterprise Information Environment. See Reference (j).

E2.30. Global Information Grid (GIG). See Reference (c).

E2.31. Impact Code. For the purpose of this Instruction, a code indicating the consequences of a non-compliant IA control. It is an indicator of the impact associated with exploitation of the IA control. In conjunction with the severity category, it also indicates the urgency with which corrective action should be taken. Impact codes are expressed as high, medium, and low, with high indicating the greatest impact.

E2.31.1. High Impact Code. The absence or incorrect implementation of the IA control may have a severe or catastrophic effect on system operations, management, or information sharing. Exploitation of the weakness may result in the destruction of information resources and/or the complete loss of mission capability.

E2.31.2. Medium Impact Code. The absence or incorrect implementation of the IA control may have a serious adverse effect on system operations, management, or information sharing. Exploitation of the weakness may result in loss of information resources and/or the significant degradation of mission capability.

E2.31.3. Low Impact Code. The absence or incorrect implementation of the IA control may have a limited adverse effect on system operations, management, or information sharing. Exploitation of the weakness may result in temporary loss of information resources and/or limit the effectiveness of mission capability.

E2.32. Implementation Procedures. Procedures describing the required steps and providing guidance for implementing DoD IA controls. Implementation procedures are found in the DIACAP KS.

E2.33. Information Assurance (IA). See Joint Publication 1-02 (Reference (w)).

E2.34. Information Assurance Control. See Reference (b).

E2.35. Information Assurance Manager (IAM). See Reference (d).

E2.36. Information Assurance Officer (IAO). See Reference (d).

E2.37. Information Assurance Support Environment. See Reference (d).

E2.38. Information Owner. See Reference (v).

E2.39. Information Resources. See Reference (w).

E2.40. Information System (IS). See Reference (d).

E2.41. Information System Security Engineering. See Reference (d).

E2.42. Interim Authorization to Operate (IATO). A temporary authorization to operate a DoD IS under the conditions or constraints enumerated in the accreditation decision.

E2.43. Interim Authorization to Test (IATT). A temporary authorization to test a DoD IS in a specified operational information environment or with live data for a specified time period within the timeframe and under the conditions or constraints enumerated in the accreditation decision.

E2.44. IT Security Plan of Action and Milestones (POA&M). A permanent record that identifies tasks to be accomplished in order to resolve security weaknesses. Required for any accreditation decision that requires corrective actions, it specifies resources required to accomplish the tasks enumerated in the plan and milestones for completing the tasks. Also used to document DAA-accepted non-compliant IA controls and baseline IA controls that are not applicable. An IT Security POA&M may be active or inactive throughout a system's life cycle as weaknesses are newly identified or closed.

E2.45. Mission Area (MA). See Reference (j).

E2.46. Mission Assurance Category (MAC). See Reference (b).

E2.47. Net-centric. See DoDD 8320.2 (Reference (x)).

E2.48. Platform IT Interconnection. See Reference (d).

E2.49. Principal Accrediting Authority (PAA). The senior official representing the interests of a GIG MA regarding C&A. Also issues C&A guidance specific to a GIG MA as required.

E2.50. Program Manager or System Manager (PM or SM). For the purpose of this Instruction, the individual with responsibility for and authority to accomplish program or system objectives for development, production, and sustainment to meet the user's operational needs.

E2.51. Proxy. See Reference (b).

E2.52. Residual Risk. See Reference (v).

E2.53. Security Relevant Event. For the purpose of this Instruction, an event that could cause a harmful change in an IS or its environment, or that an IAM would consider worthy of notation, investigation, or prevention (e.g., the discovery of malicious code in an IS, the discovery of an attempt to connect an unapproved device to the network).

E2.54. Senior Information Assurance Officer (SIAO). The official responsible for directing an organization's IA program on behalf of the organization's chief information officer.

E2.55. Service-Oriented Architecture. For the purpose of this Instruction, a paradigm for defining, organizing, and using distributed capabilities in the form of loosely coupled software services that may be under the control of different ownership domains. It provides a uniform means to offer, discover, interact with, and use capabilities to produce desired effects that are consistent with measurable preconditions and expectations.

E2.56. Severity Category. The category a CA assigns to a system security weakness or shortcoming as part of a certification analysis to indicate the risk level associated with the security weakness and the urgency with which the corrective action must be completed. Severity categories are expressed as “Category (CAT) I, CAT II, or CAT III,” with CAT I indicating the greatest risk and urgency. Severity categories are assigned after consideration of all possible mitigation measures that have been taken within system design/architecture limitations for the DoD IS in question.

E2.56.1. CAT I Severity Category. Assigned to findings that allow primary security protections to be bypassed, allowing immediate access by unauthorized personnel or unauthorized assumption of super-user privileges. An ATO will not be granted while CAT I weaknesses are present.

E2.56.2. CAT II Severity Category. Assigned to findings that have a potential to lead to unauthorized system access or activity. CAT II findings that have been satisfactorily mitigated will not prevent an ATO from being granted.

E2.56.3. CAT III Severity Category. Assigned findings that may impact IA posture but are not required to be mitigated or corrected in order for an ATO to be granted.

E2.57. Stand-Alone Information System. An information system operating independently of and without interconnection to any other information system.

E2.58. System Identification Profile (SIP). A compiled list of system characteristics or qualities required to register an IS with the governing DoD Component IA program.

E2.59. User Representative (UR). An individual or organization that represents the user community for a particular system for DIACAP purposes.

E2.60. Validation. Activity applied throughout the system’s life cycle to confirm or establish by testing, evaluation, examination, investigation, or competent evidence that a DoD IS’s assigned IA controls are implemented correctly and are effective in their application.

E2.61. Validation Procedure. Preparatory steps and conditions, actual validation steps, expected results, and criteria and protocols for recording actual results that are used for validating IA controls. May include associated supporting background material, sample results, or links to automated testing tools.

E2.62. Validator. Entity responsible for conducting a validation procedure.

E2.63. Web Services. Self-describing, self-contained, modular units of software application logic that provide defined business functionality. Web services are consumable software services that typically include some combination of business logic and data. Web services can be aggregated to establish a larger workflow or business transaction. Inherently, the architectural components of Web services support messaging, service descriptions, registries, and loosely coupled interoperability.



E3. ENCLOSURE 3THE DIACAP PACKAGE

E3.1. The DIACAP package is developed through DIACAP activity and maintained throughout a system's life cycle. Implementing the activities of the DIACAP generates the results listed in the "Comprehensive Package" column of Table E3.T1. The "Executive Package" column lists the minimum information necessary for an accreditation decision. Note that Table E3.T1. is not meant to describe a single fixed document format. Each DAA will determine what information is necessary to make an accreditation decision.

Table E3.T1. DIACAP Package Contents

<b>Comprehensive Package</b>	<b>Executive Package</b>
System Identification Profile (SIP)	SIP
DIACAP Implementation Plan (DIP) <ul style="list-style-type: none"> <li>• IA controls – inherited and implemented</li> <li>• Implementation status</li> <li>• Responsible entities</li> <li>• Resources</li> <li>• Estimated completion date for each IA control</li> </ul>	
Supporting Certification Documentation <ul style="list-style-type: none"> <li>• Actual validation results</li> <li>• Artifacts associated with implementation of IA controls</li> <li>• Other</li> </ul>	
DIACAP Scorecard <ul style="list-style-type: none"> <li>• Certification determination</li> <li>• Accreditation decision</li> </ul>	DIACAP Scorecard <ul style="list-style-type: none"> <li>• Certification determination</li> <li>• Accreditation decision</li> </ul>
IT Security POA&M (If required)	IT Security POA&M (If required)

E3.2. The SIP is compiled during the DIACAP registration and maintained throughout the system life cycle. An overview of the SIP is provided in Attachment 1 to Enclosure 3.

E3.3. The DIACAP Scorecard is a summary report that conveys information on the IA posture of a DoD IS succinctly in a format that can be exchanged electronically. A notional scorecard is provided in Attachment 2 to Enclosure 3. Additional data elements may be specified by CIOs, DAAs, or other enterprise users of the DIACAP Scorecard.

E3.4. An IT Security POA&M is required for any accreditation decision that requires corrective action and is also used to document NC or NA IA controls that have been accepted by the responsible DAA. The IT Security POA&M addresses:

E3.4.1. Why the system needs to operate.

E3.4.2. Any operational restrictions imposed to lessen the risk during an interim authorization.

E3.4.3. The DAA's rationale for accepting certain IA controls that are categorized as NC or NA.

E3.4.4. Specific corrective actions necessary to ensure that assigned IA controls have been implemented correctly and are effective.

E3.4.5. The agreed-upon timeline for completing and validating corrective actions.

E3.4.6. The resources necessary and available to properly complete the corrective actions. Attachment 3 to Enclosure 4 provides instructions for understanding and developing an IT Security POA&M.

Attachments – 3

E3.A1. System Identification Profile

E3.A2. Notional DIACAP Scorecard

E3.A3. IT Security POA&M Instructions

E3.A1. ATTACHMENT 1 TO ENCLOSURE 3SYSTEM IDENTIFICATION PROFILE

E3.A1.1. The SIP identifies the data requirements for registering an IS with the governing DoD Component IA program. Information requirements for the SIP are described in Table E3.A1.T1.

Table E3.A1.T1. System Identification Profile

<b>ID</b>	<b>Data Element Descriptor</b>	<b>Example, Acceptable Values or Comment</b>	<b>Required/Conditional<sup>1</sup></b>
1	System Identification	The System Identification Number or Code used by the DoD Component to uniquely identify the system.	Required/System Generated
2	System Owner	List the element or organization within the DoD Component that owns, controls, or manages the IS.	Required
3	Governing DoD Component IA Program	List the DoD Component that owns the IS.	Required
4	System Name	Provide the full descriptive name, e.g., Agency Billing System.	Required
5	Acronym	Provide a shortened or commonly used name or abbreviation (upper case) for this entry (e.g., ABS).	Required
6	System Version or Release Number	List the version or release number for the IS (e.g., 1.0).	Required
7	System Description	Provide a narrative description of the system, its function, and uses. Indicate if the system is stand-alone.	Required
8	DIACAP Activity	Identify the current DIACAP Activity: <ol style="list-style-type: none"> <li>1. Initiate and plan IA C&amp;A</li> <li>2. Implement and validate assigned IA controls</li> <li>3. Make certification determination and accreditation decision</li> <li>4. Maintain ATO and conduct reviews</li> <li>5. Decommission</li> </ol>	Required

Table E3.A1.T1. System Identification Profile, (cont'd)

<b>ID</b>	<b>Data Element Descriptor</b>	<b>Example, Acceptable Values or Comment</b>	<b>Required/Conditional<sup>1</sup></b>
9	System Life Cycle Phase	Identify the current life-cycle phase of the information system: <ol style="list-style-type: none"> <li>1. Concept Refinement</li> <li>2. Technology Development</li> <li>3. System Development and Demonstration</li> <li>4. Production and Deployment</li> <li>5. Operations and Support</li> <li>6. Disposal or Decommissioning</li> </ol>	Required
10	System Acquisition Phase	For programs of record, identify the current System Acquisition Phase: <ol style="list-style-type: none"> <li>1. Pre-Milestone A (Concept Refinement)</li> <li>2. Post-Milestone A (Technology Development)</li> <li>3. Post-Milestone B (System Development and Demonstration)</li> <li>4. Post-Milestone C (Production and Deployment)</li> <li>5. Post-Full Rate Production/Deployment Decision (FRPD/FRDD)</li> </ol>	Conditional
11	IA Record Type	Identify the type of DoD information system (i.e., AIS Application, Enclave*, Outsourced IT-Based Process** or Platform IT Interconnection).  *Indicate if stand-alone or DMZ. ** Indicate if DoD-controlled or control shared with service provider.	Required
12	Mission Criticality	Identify the mission criticality of this system (i.e., mission critical (MC), mission essential (ME), or mission support (MS) if neither MC or ME. (Reference (1)).	Required
13	Accreditation Vehicle	Identify the C&A process that was or is being used to C&A the IS (e.g., DIACAP, DCID 6/3, NIST 800-37).	Required
14	Additional Accreditation Requirements	Identify any additional accreditation requirements beyond the IA C&A process (e.g., privacy, special access requirements (SAR), cross security domain solutions, Non Classified Internet Protocol Router Network (NIPRNet), Secret Internet Protocol Router Network (SIPRNet), or GIG CAP identifier, ports, protocols, and services management.)	Conditional

Table E3.A1.T1. System Identification Profile, (cont'd)

<b>ID</b>	<b>Data Element Descriptor</b>	<b>Example, Acceptable Values or Comment</b>	<b>Required/Conditional<sup>1</sup></b>
15	ACAT Category	Identify the acquisition category if applicable according to Reference (1) (e.g., ACAT I).	Conditional
16	Governing Mission Area	Enterprise Information Environment MA (EIEMA), Business MA (BMA), Warfighting MA (WMA), or Defense Intelligence MA (DIMA)	Required
17	Software Category	Identify whether the system software is commercial off-the-shelf (COTS) or Government off-the-shelf (GOTS).	Required
18	MAC Level	List the information system's MAC level (i.e., MAC I, MAC II, or MAC III).	Required
19	Confidentiality Level	List the information system's CL (i.e., public, sensitive, or classified).	Required
20	Accreditation Status	Identify the accreditation status of the IS (i.e., unaccredited, ATO, IATO, IATT, DATO).	Required (default is unaccredited)
21	Certification Date	List the date the IS was certified by the CA.	Conditional
22	Accreditation Documentation	Are there documentation and artifacts that support the accreditation status? Answer Yes or No.	Conditional
23	Accreditation Date	List the date of the current accreditation decision (ATO, IATO, IATT, DATO). If the IS has no accreditation determination, enter "NONE" and the projected accreditation date.	Required
24	Authorization Termination Date	List the date that the current accreditation (ATO, IATO, IATT) is set to expire.	Conditional
25	DIACAP Team Roles, Member Names, and Contact Information	Identify the DIACAP Team (e.g., DAA, the CA, the DoD IS PM or SM, the DoD IS IAM, IAO, and UR).	Required

Table E3.A1.T1. System Identification Profile, (cont'd)

<b>ID</b>	<b>Data Element Descriptor</b>	<b>Example, Acceptable Values or Comment</b>	<b>Required/Conditional<sup>1</sup></b>
26	Privacy Impact Assessment Required	Indicate whether a privacy impact assessment is required for a new or previously existing IT system. Reference DoD 5400.11-R (Reference (y)). Answer Yes or No.	Required
27	Privacy Act System of Records Notice Required	Indicate whether a Privacy Act System of Record Notice is required by Reference (y). Answer Yes or No.	Required
28	E-Authentication Risk Assessment Required	Indicate whether an E-Authentication Risk Assessment has been performed for the system according to OMB M-04-04 (Reference (z)). Answer Yes or No.	Required
29	Date of Annual Security Review	List the date of the last annual security review for systems with an ATO. Required by Reference (a) and by the DIACAP for ISs with an ATO in effect for more than 1 year.	Required
30	System Operation	Identify whether the system operation is: 1. Government (DoD) Owned, Government Operated (GOGO) 2. Government (DoD) Owned, Contractor Operated (GOCO) 3. Contractor Owned, Contractor Operated (COCO) – includes outsourced IT services 4. Contractor Owned, Government (DoD) Operated (COGO) 5. Non-DoD – includes Federal, State, and local governments, grantees, industry partners, etc.	Required
31	Contingency Plan Required	Indicate whether a contingency plan addressing disruptions in operations of the IS is in place. Answer Yes or No.	Required
32	Contingency Plan Tested	Indicate whether the contingency plan that is in place has been tested. Answer Yes or No.	Required

<sup>1</sup> Required entries are mandatory for completing the SIP. Conditional entries must be completed if they apply to the system being profiled. If the entry does not apply, the box is left blank.

E3.A2. ATTACHMENT 2 TO ENCLOSURE 3DIACAP SCORECARD

E3.A2.1. The DIACAP Scorecard is a summary report that succinctly conveys information on the IA posture of a DoD IS in a format that can be exchanged electronically. It documents the accreditation decision and must be signed, either manually or with a DoD PKI-certified digital signature. The DIACAP Scorecard contains a listing of all IA controls and their status of either C, NC, or NA. An example of a DIACAP Scorecard is shown in Figure E3.A2.F1. Table E3.A2.T1. explains the fields contained in Figure E3.A2.F1.

Figure E3.A2.F1. Example of a DIACAP Scorecard**DIACAP SCORECARD**

System Name <b>Enterprise Mission Assurance Support Service</b>		System Owner <b>ASD(NII)</b>		IS Type <b>AIS Application</b>	
Designated Accrediting Authority (DAA) <b>Nathan Gray</b>		Accreditation Status <b>ATO</b>	Accreditation Date <b>23-Sep-05</b>	Period Covered ATD <b>23-Sep-07</b>	Last Update <b>24-Dec-05</b>
Certifying Authority (CA) <b>Matthew Summers</b>		Certification Date <b>10-Sep-05</b>	Mission Assurance Category (MAC) <b>MAC II</b>		Confidentiality Level (CL) <b>Sensitive</b>

☐ MAC I, Classified   ☐ MAC II, Classified   ☐ MAC III, Classified  
☐ MAC I, Sensitive   ☒ MAC II, Sensitive   ☐ MAC III, Sensitive  
☐ MAC I, Public   ☐ MAC II, Public   ☐ MAC III, Public

IA Control Subject Area	IA Control Number	IA Control Name	Inherited?	C/NC/NA	Impact Code	Last Update
Continuity	COAS-2	Alternate Site Designation	No	C	Medium	02-Nov-05
Continuity	COBR-1	Protection of Backup and Restoration Assets	No	C	High	02-Nov-05
Continuity	CODB-2	Data Back-up Procedures	Yes	C	Low	30-Sep-05
Continuity	CODP-2	Disaster and Recovery Planning	No	NC	Medium	08-Nov-05
Continuity	COEB-1	Enclave Boundary Defense	Yes	C	High	02-Nov-05
Continuity	COED-1	Scheduled Exercises and Drills	No	C	Medium	24-Dec-05

Table E3.A2.T1. Scorecard Instructions

Reference	Description
System Name	The name of the system being certified.
System Owner	The organization within the DoD Component that owns, controls, or manages the IS.
IS Type	The IS type (i.e., AIS application, enclave, outsourced IT-based process, and platform IT interconnection). Indicate if the enclave is stand-alone or a DMZ.
DAA	The name and signature of the DAA for the system. Manual or DoD PKI-certified digital signatures are acceptable.

Table E3.A2.T1. Scorecard Instructions, (cont'd)

Reference	Description
Accreditation Status	The accreditation decision for the system (i.e., unaccredited, ATO, IATO, IATT, DATO).
Period Covered	Includes the date of the accreditation (if the system has a decision other than unaccredited), and the ATD.
Last Update	The date of the last change that occurred on the scorecard. This is primarily driven by updates to the IA controls and their associated status.
CA	The name of the individual serving as the CA for the system.
Certification Date	The date of the certification.
MAC	The MAC applied to the system.
CL	The CL applied to the system.
IA Control Subject Area	The subject area associated with the IA control.
IA Control Number	The reference number associated with the IA control.
IA Control Name	The name associated with the IA control.
Inherited	An indication (Yes or No) of whether or not the IA control is inherited.
C/NC/NA	An indication of the compliance status of the IA control (i.e., C, NC, NA). An IT Security POA&M is required if NC or NA. Note: NC may indicate either non-implementation or complete failure of the control under testing; it also may indicate a partial failure of a control under testing (e.g., three of four testing points pass).
Impact Code	The impact code associated with the IA control.
Last Update	The date of the last change of the IA control's compliance status (C/NC/NA).



**E3.A3. ATTACHMENT 3 TO ENCLOSURE 3**

**IT SECURITY POA&M INSTRUCTIONS**

E3.A3.1. The primary purpose of an IT Security POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring security weaknesses found in programs and systems, along with the progress of corrective efforts for those vulnerabilities. OMB requires agencies to prepare IT Security POA&Ms for all programs and systems in which an IT security weakness has been found. OMB guidance (Reference (aa)) directs CIOs and the DoD Component program officials to develop, implement, and manage IT Security POA&Ms for all programs and systems they operate and control (for program officials this includes all systems that support their operations and assets, including those operated by contractors). In addition, program officials are required to update the agency CIO on their progress on at least a quarterly basis and at the direction of the CIO. This enables the CIO to monitor agency-wide remediation efforts and provide the agency's quarterly update to OMB. Under the DIACAP, the IT Security POA&M is also used to document DAA-accepted non-compliant IA controls and baseline IA controls that are not applicable because of the nature of the system (e.g., stand-alone systems).

E3.A3.2. The IT Security POA&M is designed to be a management tool to assist: agencies in closing their security performance gaps; IGs in their evaluation work of agency security performance; and OMB with oversight responsibilities. The Department of Defense is responsible for maintaining the confidentiality of IT Security POA&Ms because they may contain pre-decisional budget information. There are three types of IT Security POA&Ms, as reflected in Table E4.A3.T1. DoD IT Security POA&Ms shall:

E3.A3.2.1. Be tied to the agency's budget submission when required through the project identifier(s) of the system. This links the security costs with security performance. OMB Circular No. A-11 (Reference (ab)) requires that agencies develop and submit to OMB business cases (Exhibits 300) for major IT investments. Additionally, each agency submits an Exhibit 53, a list of both major and non-major IT investments. The agency assigns project identifier(s) to each investment and includes it with these exhibits.

E3.A3.2.2. Address all IT security weaknesses, including but not limited to those found during GAO audits, financial system audits, official security tests and evaluations or compliance reviews, and critical infrastructure vulnerability assessments.

E3.A3.2.3. Be shared with the agency IG to ensure independent verification and validation of identified weaknesses and completed corrective actions.

E3.A3.2.4. Follow the format detailed below that is consistent with the examples provided by OMB.

E3.A3.2.5. Be submitted to the DoD SIAO when directed.

Table E3.A3.T1. Types of DoD IT Security POA&Ms

Report	Responsibility	Submit To	Dates Due
System-level IT Security POA&Ms (Table E4.A3.T2)	PMs/IAMs	DoD Component CIO  (Also to DoD SIAO for all systems with a CAT I weakness or on the OMB Watch List (Exhibit 300s) for security)	1 Dec, 1 Mar, 1 Jun, 1 Sep
DoD Component-level IT Security POA&M (Table E4.A3.T3)	DoD Component CIO	ASD(NII)/DoD CIO	Due with the DoD Component's annual FISMA report and as directed
DoD Enterprise IT Security POA&M	ASD(NII)/DoD CIO	OMB	As directed

E3.A3.3. The subparagraphs below describe the System Level IT Security POA&M.

E3.A3.3.1. The DoD Component CIOs are responsible for monitoring and tracking the overall execution of system-level IT Security POA&Ms until identified security weaknesses have been closed and the C&A documentation appropriately adjusted. The DAAs are responsible for monitoring and tracking overall execution of system-level IT Security POA&Ms. The PM or SM is responsible for implementing the corrective actions identified in the IT Security POA&M and, with the support and assistance of the IAM, provides visibility and status to the DAA, the SIAO, and the governing DoD Component CIO.

E3.A3.3.2. Table E3.A3.T2. is an example of a completed system-level IT Security POA&M, illustrating the appropriate level of detail required. Included in the heading of the system-level IT Security POA&M template is a field for OMB Project ID and Security Costs, which must be filled in from Exhibits 300 and 53, where applicable.

E3.A3.3.3. Once an initial system-level IT Security POA&M weakness has been opened, changes cannot be made to the data in columns 1 ("Weakness"), 6 ("Scheduled Completion Date"), 7 ("Milestones with Completion Dates"), and 9 ("Source Identifying Weakness").

E3.A3.3.4. IT Security POA&Ms listing CAT I or CAT II weaknesses shall be assessed for classification. For instance, the fact that a MAC I or MAC II IS has a CAT I weakness that has not been mitigated to a degree that will preclude immediate unauthorized access dictates a minimum classification of CONFIDENTIAL. Other factors that would influence a classification decision include the number of CAT II weaknesses identified for a single system and whether the system itself is classified. At a minimum an IT Security POA&M will be protected as Sensitive. Classified IT Security POA&Ms for unclassified systems must be maintained in an appropriate environment separate from the unclassified DIACAP Package.

E3.A3.4. The following sections explain how to complete the system-level IT Security POA&M fields. Note: NA IA controls will have entries only in columns 1, 3, and 11.

E3.A3.4.1. Column 1: Type of Security Weakness. Describe security weaknesses identified during certification or by the annual program review, independent evaluations by IGs, or any other work done by or on behalf of the program office or the DoD Component. Sensitive descriptions of specific weaknesses are not necessary, but sufficient data must be provided to permit oversight and tracking. When it is necessary to provide more sensitive data, the IT Security POA&M should note the fact of its special sensitivity and it should be protected accordingly. When more than one weakness has been identified, number each individual security weakness as shown in the examples. Indicate “NA” in this column as required.

E3.A3.4.2. Column 2: CAT (Severity Category). Category assigned to a system IA security weakness by a CA as part of certification analysis to indicate the risk level associated with the IA security weakness and the urgency with which the corrective action must be completed. Severity categories are expressed as CAT I, CAT II, or CAT III, with CAT I indicating the greatest risk and urgency.

E3.A3.4.3. Column 3: IA Control and Impact Code. An IA control describes an objective IA condition achieved through the application of specific safeguards or through the regulation of specific activities. The objective condition is testable, compliance is measurable, and the activities required to achieve the IA control are assignable and thus accountable. IA controls are assigned according to MAC (for integrity and availability) and CL in accordance with Reference (d). Impact codes indicate the consequences of a non-compliant IA control and are expressed as high, medium, or low, with high indicating the greatest impact.

E3.A3.4.4. Column 4: Point of Contact (POC). Identity the office or organization that the DoD Component will hold responsible for resolving the security weakness.

E3.A3.4.5. Column 5: Resources Required. Estimated funding or manpower (i.e., full-time equivalents) resources required to resolve the security weakness. Enter “NA” for CAT III weaknesses accepted by the DAA.

E3.A3.4.6. Column 6: Scheduled Completion Date. Scheduled completion date for resolving the security weakness. Please note that the initial date entered should not be changed. If a security weakness is resolved before or after the originally scheduled completion date, the agency should note the actual completion date in column 10 (“Status”). Enter “NA” if risk is accepted for a satisfactorily mitigated CAT II or a CAT III weakness.

E3.A3.4.7. Column 7: Milestones with Completion Dates. A milestone will identify specific requirements for correcting an identified weakness. Please note that the initial milestones and completion dates should not be altered. If there are changes to any of the milestones, the agency should note them in column 8 (“Milestone Changes”). Enter “NA” for CAT III weaknesses accepted by the DAA.

E3.A3.4.8. Column 8: Milestone Changes. This column includes changes to completion dates and reasons for the changes. Enter “NA” for CAT III weaknesses accepted by the DAA.

E3.A3.4.9. Column 9: Source Identifying the Weakness. Identify the source (e.g., program review, test and evaluation program findings, IG DoD audit, GAO audit) of the security weakness.

E3.A3.4.10. Column 10: Status. The DoD Component should use one of the following terms to report status of corrective actions: ongoing, completed, or risk accepted for a CAT II or CAT III weakness that has been accepted by the DAA. “Completed” should be used only when a security weakness has been fully resolved and the corrective action has been tested. Include the date of completion or risk acceptance for a CAT III weakness. Enter “Risk Accepted by DAA” for CAT III weaknesses accepted by the DAA.

E3.A3.4.11. Column 11: Comments. If the IA control is inherited, cite the originating IS. For NA IA controls, provide the reason the control is not applicable. Additional information may include anticipated source of funding and other obstacles and challenges to resolving the security weakness (e.g., lack of personnel or expertise, development of new system to replace insecure legacy system).

Table E3.A3.T2. System-Level IT Security POA&amp;M Example

System Level IT Security POA&M Example										
Date Initiated:	October 1, 2005			IS Type:	Enclave			OMB Project ID:	009-222334-55874	
Date Last Updated:	January 10, 2006			(See Note 1)			(See Note 2)			
Component Name	OSD			POC Name:	James Avery					
System / Project Name:	DoD Network			POC Phone:	703-698-7753			Security Costs:	(See Note 3) \$62,500	
DoD IT Registration No:	86753			POC E-Mail:	<a href="mailto:james.avery@dod.ctr.mil">james.avery@dod.ctr.mil</a>					
Weakness (1) (See Note 4)	CAT (2)	IA Control and Impact Code (3)	POC (4)	Resources Required (5)	Scheduled Completion Date (6)	Milestones with Completion Dates (7)	Milestone Changes (8)	Source Identifying Weakness (9)	Status (10)	Comments (11)
1 An account management process has not been implemented to ensure that only authorized users can gain access to the DoD network and that individual accounts designated as inactive, suspended, or terminated are promptly deactivated.	I	IAAC-1 Impact High	IAO	\$50,000	5/30/2005	Develop an account Management Process - 1/15/2005; Management Review of account management process 3/15/2005; Implement/Test account management process - 4/15/2005	Implementing and Testing the account management process delayed till 10/15/2005 due to inadequate funding	8500.2 IA Controls Test Conducted 5/15/2005	Ongoing	Funding will be available in FY 2006
2 Security plan is out of date, more than one year since last update despite new interconnections	II	DCSD-1 Impact High	IAO	\$5,000	11/30/2005	Update plan and obtain independent review - 11/30/2005		8500.2 IA Controls Test Conducted 5/15/2005	Ongoing	
3 Lack of accurate systems hardware and software baseline hampers implementation of Configuration Management processes.	II	DCHW-1/DCSW-1 Impact High	IAO	\$0	8/31/2005	Establish baseline inventory of the hardware and software and utilize revision control system - 6/15/2005. Implement a software revision control program - 8/31/2005		Security Test and Evaluation - 4/15/2005	Completed - 10/30/2005	
4 Encryption is not certified FIPS 140-2 compliant.	III	DCNR-1 Impact Medium	IAO	\$5,000	10/21/2005	Upgrade encryption software to FIPS 140-2 certified version 10/21/2005		IG Audit 3/21/2005	Ongoing	May slip due to delay in funding
5										
6										
7										
8										
9										
10										
11										

Note 1 – Indicate if the enclave is stand-alone or a DMZ.

Note 2 – Cite project identifier(s) from OMB Exhibit 300, if applicable.

Note 3 – Security costs from OMB Exhibit 53, if applicable.

Note 4 – NA IA controls will have entries only in columns 1, 3, and 11.

E3.A3.5. The subparagraphs below describe the DoD Component-Level IT Security POA&M.

E3.A3.5.1. DoD Components are required to complete and submit a DoD Component-level IT Security POA&M as indicated in Table E3.A3.T1. A DoD Component-level IT Security POA&M is required for the following:

E3.A3.5.1.1. Systemic weaknesses (significant IA security weaknesses) identified across the DoD Component.

E3.A3.5.1.2. Systemic weaknesses (significant IA security weaknesses) identified by GAO and IG DoD audits and reviews.

E3.A3.5.2. Table E3.A3.T3. contains an example of a completed DoD Component-level IT Security POA&M, illustrating the appropriate level of detail required. Once a DoD Component has completed the initial DoD Component-level IT Security POA&M, no changes should be made to the data in columns 1 (“Weakness”), 4 (“Scheduled Completion Date”), 6 (“Milestones with Completion Dates”), and 8 (“Identified in GAO Audit or Other Review”).

E3.A3.5.3. Refer to the instructions for the system-level IT Security POA&M in section E3.A3.4. for guidance in filling out applicable items on the DoD Component-level POA&M.

Table E3.A3.T3. The DoD Component-Level IT Security POA&M Example

Component Level IT Security POA&M Example								
Date:		March 1, 2005		POC Name:		Mr. Navy CIO		
Component Name:		DON		POC Phone:		555-555-5555		
				POC E-mail:		<a href="mailto:doncio@nav.mil">doncio@nav.mil</a>		
Weakness (1)		POC (2)	Resources Required (3)	Scheduled Completion Date (4)	Milestones with Completion Dates (5)	Milestone Changes (6)	Source Identifying Weakness (7)	Status (8)
1	Annual testing of contingency plans not being conducted	Component CIO	700K	3/1/2006	Verify and test contingency plans for 98% of systems C&A 12/30/05		Annual Review	Ongoing
2	Security Awareness, Training, and Education – no process for tracking completion of specialized training	Component CIO	200K	10/1/2005	Implement and test training database 6/1/05  Enter personnel requiring specialized training into database 10/1/05		OIG Audit	Ongoing
3	Inconsistent and inadequate personal computer inventory afloat	Component CIO	500K	10/1/2006	Implement and test afloat computer inventory system 10/1/05  Enter 50% afloat inventory into database 3/1/06		Naval Audit Service	Ongoing

E3.A3.6. The subparagraphs below describe the DoD Enterprise-Level IT Security POA&M.

E3.A3.6.1. The DoD CIO is responsible for completing and submitting a DoD Enterprise-level IT Security POA&M as indicated in Table E3.A3.T1.

E3.A3.6.2. Systemic IA security weaknesses reported on the DoD Enterprise-level IT Security POA&M are derived from the DoD Component-level IT Security POA&Ms, GAO and IG DoD audits, and other reviews and events.



#### E4. ENCLOSURE 4

##### DIACAP KNOWLEDGE SERVICE (KS)<sup>1</sup> OVERVIEW

E4.1. DoD IA practitioners and developers need ready access to current DIACAP implementation guidance in order to uniformly apply the methods, standards, and practices required to successfully certify and accredit the DoD ISs comprising the GIG. Because the GIG is an ever-changing entity, DoD IA practitioners tasked with GIG certification and accreditation responsibilities require implementation guidance, access, and content suitable to accomplishing C&A in this dynamic DoD-wide environment. Implementation guidance must reflect the most up-to-date DoD intent regarding evolving IA security objectives and risk conditions. Written manuals that must be formally and laboriously coordinated lack the timeliness and versatility required to adequately meet the access, distribution, and relevancy challenges posed. To address this enterprise challenge, the DIACAP KS, developed and owned by the Department of Defense, has been established as the on-line, Web-based resource that provides requirements, guidance, and tools for implementing and executing the DIACAP. The KS is available to all individuals with C&A responsibilities, provides convenient access to Reference (d) IA controls and required standardized IA control implementation and validation procedures, and assists members of the IA community in fulfilling the requirements of the DIACAP. It is accessible by individuals with a DoD PKI certificate (Common Access Card (CAC)), or External Certification Authority (ECA) certificate in conjunction with DoD sponsorship (e.g., for DoD contractors without a CAC and working off-site). The KS is the DoD official resource for implementing and executing the DIACAP.

E4.2. The purpose of the DIACAP KS is to provide IA practitioners and managers with a single authorized source for execution and implementation guidance, community forums, and the latest information and developments in DIACAP. The DIACAP KS supports both automated and non-automated implementation of the DIACAP.

E4.3. The KS is a library of tools, diagrams, process maps, documents, etc., to support and aid in the execution of the DIACAP. It is a collaboration workspace for the DIACAP user community to develop, share, and post lessons learned and best practices and a source for IA news and events and other IA-related information resources.

E4.4. The DIACAP TAG is responsible for maintaining CCM of the online KS content. The TAG:

E4.4.1. Provides detailed analysis and authoring support for the enterprise portion of the DIACAP KS content.

---

<sup>1</sup> <https://diacap.iaportal.navy.mil/>

E4.4.2. Provides configuration control for DIACAP-related enterprise services, including DIACAP KS functionality.

E4.4.3. Interfaces with the DoD Component IA programs, GIG MAs, IA COIs, and specialized entities within the IA domain governance structure. (See Figure F1.)

E4.4.4. Addresses issues that are common across entities and recommends changes to the baseline IA controls and C&A process.

E5. ENCLOSURE 5DIACAP TRANSITION TIMELINE AND INSTRUCTIONS

E5.1. The DIACAP Transition Timeline and Instructions provide guidance and direction for all systems transitioning to DIACAP from the DITSCAP environment.

Table E5.T1. DIACAP Transition Timeline and Instructions

<b>DoD IS C&amp;A STATUS</b>		<b>TRANSITION TIMELINE and INSTRUCTIONS</b>
1	Unaccredited new start or operational DoD IS (No DITSCAP activity).	Initiate DIACAP.
2	DoD IS has initiated DITSCAP, but does not yet have a signed Phase One System Security Authorization Agreement (SSAA).	Transition to DIACAP immediately.
3	DoD IS has a DITSCAP Phase One signed SSAA and is in Phase Two or Phase Three (does not yet have an accreditation decision). The Phase One SSAA Requirements Traceability Matrix (RTM) incorporates all DoD baseline IA controls as specified in Reference (d).	Continue under DITSCAP. The DITSCAP SSAA section addressing re-accreditation requirements (section 5.7 in the SSAA outline of Reference (e)) should have been modified as directed by Reference (g) to identify the governing DoD Component IA program and describe the system's strategy and schedule for transitioning to DIACAP, satisfying the DIACAP Annual Review and meeting the reporting requirements of FISMA (Reference (a)).  The schedule for transitioning from DITSCAP to DIACAP shall not exceed the system re-accreditation timeline.
4	DoD IS has a DITSCAP Phase One signed SSAA and is in Phase Two or Phase Three (does not yet have an accreditation decision). The Phase One SSAA RTM does not incorporate all DoD baseline IA controls as specified in Reference (d).	Comply with guidance at #3 above and continue under DITSCAP. The DITSCAP RTM to incorporate all DoD baseline IA controls as specified in Reference (d) and a plan for implementing them should have been modified as directed by Reference (g). IA controls implementation timelines

Table E5.T1. DIACAP Transition Timeline and Instructions, (cont'd)

<b>DoD IS C&amp;A STATUS</b>		<b>TRANSITION TIMELINE and INSTRUCTIONS</b>
		may extend beyond the DITSCAP accreditation decision, that is, the DITSCAP accreditation decision is not contingent upon full compliance with the baseline IA controls, but the system must provide information/visibility of its compliance status and have a viable plan for achieving compliance in order to be granted an accreditation decision under DITSCAP.
5	DoD IS has a DITSCAP accreditation decision that is current within 3 years.	<p>A strategy and schedule for transitioning to DIACAP, achieving compliance with Reference (d) baseline IA controls, satisfying the DIACAP Annual Review, and meeting the reporting requirements of Reference (a) should be completed as directed by Reference (g).</p> <p>If the DITSCAP RTM does not incorporate the baseline DoD IA controls as specified in Reference (d), the DoD IS shall provide the DAA with an assessment of compliance.</p> <p>If the accreditation decision is IATO and the system is on a path toward full authorization, continue under DITSCAP as modified by the guidelines of this table to achieve authorization.</p>
6	DoD IS has a DITSCAP ATO that is more than 3 years old.	Initiate DIACAP.



# Department of Defense INSTRUCTION

NUMBER 1402.5

January 19, 1993

ASD(FM&P)

SUBJECT: Criminal History Background Checks on Individuals In Child Care Services

References: (a) DoD 5400.11-R, "Department of Defense Privacy Program," August 1983, authorized by [DoD Directive 5400.11](#), June 9, 1982  
(b) Federal Personnel Manual, Chapter 731, "Personnel Suitability," and Chapter 736, "Personnel Investigations," September 29, 1988  
(c) DoD 5200.2-R, "DoD Personnel Security Program," January 1987, authorized by DoD Directive 5200.3, May 6, 1992  
(d) [DoD Directive 6400.1](#), "Family Advocacy Program," June 23, 1992  
(e) through (k), see enclosure 1

## 1. PURPOSE

This Instruction:

1.1. Implements Pub. L. No. 101-647, Section 231 (enclosure 3), and Pub. L. No. 102-190, Section 1094 (enclosure 4).

1.2. Requires procedures for existing and newly hired individuals and includes a review of personnel and security records to include a Federal Bureau of Investigation (FBI) fingerprint check and State Criminal History Repositories (SCHR) checks of residences listed on employment or certification applications.

1.3. Establishes policy, assigns responsibilities, and prescribes procedures for criminal history background checks for all existing and newly hired individuals involved in the provision of child care services as Federal employees, contractors, or in Federal facilities to children under the age of 18. The checks are required of all individuals in the Department of Defense involved in providing child care services defined in enclosure 3, and for policy reasons, those categories of individuals not

expressly governed by the statute.

1.4. Allows the Department of Defense to provisionally hire such individuals before the completion of a background check (enclosure 4). However, at all times while children are in the care of that individual, the child care provider must be within sight and under the supervision of a staff person whose background check has been successfully completed. Healthcare personnel shall comply with guidance provided in enclosure 5.

## 2. APPLICABILITY AND SCOPE

This Instruction:

2.1. Applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff and Unified and Specified Commands, the Inspector General of the Department of the Joint Staff, the Defense, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

2.2. Includes all individuals providing child care services to children in accordance with references (a) through (k).

## 3. DEFINITIONS

Terms used in this Instruction are defined in enclosure 2.

## 4. POLICY

It is DoD policy to:

4.1. Establish a standardized and comprehensive process for screening applicants for positions involving child care services on DoD installations and in DoD activities.

4.2. Provide fair, impartial, and equitable treatment before an individual may be deemed suitable to serve as an employee, a certified care provider, a specified volunteer position, or as an individual employed under contract in activities covered by this Instruction and references (a) through (k) by conducting a thorough review of all appropriate records as described herein.

4.3. Protect children by denying or removing from employment, contract, or volunteer status any applicant or current employee who is determined unsuitable to provide child care services because derogatory information is contained in a suitability investigation.

4.4. Ensure that an individual is advised of proposed disciplinary action, decertification, or refusal to hire by the hiring authority or designee if disqualifying derogatory information is contained in a suitability investigation. The individual is given the opportunity to challenge the accuracy and completeness of reported information.

4.5. Foster cooperation among the DoD Components, other Federal Agencies, State and county agencies, and other civilian authorities in conducting criminal history background checks.

## 5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense (Force Management and Personnel) shall:

5.1.1. Develop policy for conducting criminal history background checks on individuals seeking positions involving child care services.

5.1.2. Monitor compliance with this Instruction.

5.1.3. Coordinate oversight of criminal history background checks as specified under this Instruction.

5.2. The Heads of the DoD Components shall:

5.2.1. Develop procedures to ensure compliance with the requirements of this Instruction, in accordance with enclosure 6.

5.2.2. Provide oversight of process and procedures to conduct criminal history background checks to include assignment of proponentcy.

5.2.3. Provide technical support and resources as required.

5.2.4. Coordinate participation of specific organizations within the DoD Component involved in the conduct of the checks.

5.2.5. Ensure that applicants and employees are made aware of their rights under DoD 5400.11-R (reference (a)) including the right to challenge accuracy of records.

5.2.6. Maintain the records of all individuals hired, certified, or employed under contract for positions that involve child care services for 2 years following termination of their service.

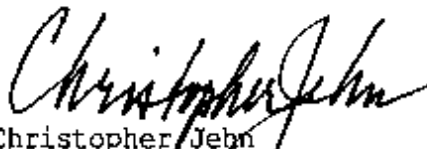
5.2.7. Establish a mechanism to evaluate all adverse information resulting from criminal history background checks, using the criteria in enclosure 7. Final suitability decisions are made by the DoD Component Head or designee.

## 6. PROCEDURES

The records of all existing employees and applicants for positions in child care services are reviewed by the Component designee according to the procedures prescribed in enclosure 6.

## 7. EFFECTIVE DATE AND IMPLEMENTATION

This Instruction is effective immediately. Forward two copies of implementing documents to the Assistant Secretary of Defense (Force Management and Personnel) within 120 days.

  
Christopher Jehn  
Assistant Secretary of Defense  
(Force Management and Personnel)

Enclosures - 8

- E1. References, continued
- E2. Definitions
- E3. Public Law 101-647, Section 231



- E4. Public Law 102-190, Section 1094
- E5. Memorandum from the Assistant Secretary of Defense Health Affairs,  
"Criminal History Background Checks on Health Care Personnel," April 20,  
1992
- E6. Criminal History Background Check Procedures
- E7. Criteria for Criminal History Background Check Disqualification
- E8. State Information

E1. ENCLOSURE 1

REFERENCES, continued

- (e) [DoD Instruction 6060.2](#), "Child Development Programs," March 3, 1989
- (f) [DoD Instruction 6400.2](#), "Child and Spouse Abuse Report," July 10, 1987
- (g) [DoD Directive 1400.13](#), "Salaries and Personnel Practices Applicable to Teachers and Other Employees of the DoD Overseas Dependents' Schools System," July 8, 1976
- (h) [DoD Directive 1342.16](#), "Provision of Free Public Education for Eligible Dependent Children Pursuant to Section 6, Public Law 81-874, as Amended," October 16, 1987
- (i) DoD Directive 6025.11, "DoD Health Care Provider Credentials Review and Clinical Privileging," May 20, 1988
- (j) [DoD Directive 1015.1](#), "Establishment, Management, and Control of Nonappropriated Fund Instrumentalities," August 19, 1981
- (k) [DoD Instruction 1000.15](#), "Private Organizations on DoD Installations," September 22, 1978

## E2. ENCLOSURE 2

### DEFINITIONS

E2.1.1. Appropriated Fund (APF) Employees. Personnel hired by DoD Components with appropriated funds as defined in the FPM, Chapter 731 (reference (b)). This includes temporary employees, 18 years old or older, who work with children.

E2.1.2. Care Provider. As defined in Pub. L. No. 101-647, Section 231 and Pub. L. No. 102-190, Section 1094 (enclosures 3 and 4). Providers included are current and prospective individuals hired with APF and nonappropriated funds (NAF) for education, treatment or healthcare, child care or youth activities, individuals employed under contract who work with children and those who are certified for care. Care providers are individuals working within programs that include alphabetically: Child Development Programs, DoD Dependents Schools, DoD-Operated or -Sponsored Activities, DoD Section 6 School Arrangements, Foster Care, Private Organizations on DoD Installations, and Youth Programs. Background checks are required for all civilian and military providers (except military healthcare providers) involved in child care services who have regular contact with children.

E2.1.3. Child. An unmarried person, whether natural child, adopted child, foster child, stepchild, or ward, who is a family member of a military member or DoD civilian or their spouse, and who is under the age of 18 years; or is incapable of self support because of a mental or physical incapacity and for whom treatment is authorized in a medical facility of the Military Services, as defined in DoD Directive 6400.1 (reference (d)).

E2.1.4. Child Abuse and/or Neglect. The physical injury, sexual maltreatment, emotional maltreatment, deprivation of necessities, or other maltreatment of a child. The term encompasses both acts and omissions on the part of a responsible person, as defined in reference (d).

E2.1.5. Child Care Services. DoD personnel and contractors who are involved in any of the following: "child protective services (including the investigation of child abuse and neglect reports), social services, health and mental health care, child (day) care, education (whether or not directly involved in teaching), foster care, residential care, recreational or rehabilitative programs, and detention, correctional, or treatment services," as defined in Pub. L. No.101-647, Section 231 (enclosure 3).

E2.1.6. Child Development Center (CDC). An installation facility or part of a facility used for child care operated under the oversight of Component's Child Development Programs (CDPs) and as defined in DoD Instruction 6060.2 (reference (e)).

E2.1.7. Child Development Programs (CDPs). Programs for dependents of DoD personnel provided in CDCs, family child care (FCC) homes, and alternative child care options. The care provided is on a full-day, part-day, or hourly basis. Care is designed to protect the health and safety of children and promote their physical, social, emotional, and intellectual development, as defined in reference (e).

E2.1.8. Child Sexual Abuse. Employment, use, persuasion, inducement, enticement, or coercion of any child to engage in, or having a child assist any other person to engage in, any sexually explicit conduct (or any simulation of such conduct) or the rape, molestation, prostitution, or any other such form of sexual exploitation of children, or incest with children. All sexual activity between an offender and a child, when the offender is in a position of power over the child, is considered sexual maltreatment, as defined in DoD Instruction 6400.2 (reference (f)).

E2.1.9. Criminal History Background Check. An investigation based on fingerprints and other identifying information obtained by a law enforcement officer conducted through the Federal Bureau of Investigation-Identification Division (FBI-ID) and SCHR of all States that an employee or prospective employee list as current and former residences on an employment application initiated through the personnel programs of the applicable Federal Agencies, as defined in Pub. L. No. 101-647 (enclosure 3) or through the personnel program of a given Government contractor.

E2.1.10. Defense Clearance and Investigations Index (DCII). The central Department of Defense record of investigative files and adjudicative actions such as clearances and access determinations, revocations, and denials concerning military, civilian, and contract personnel.

E2.1.11. DoD Dependents Schools (DoDDS). Schools operated by the Department of Defense for minor dependents of military members or DoD civilians assigned to duty in foreign countries, as defined in DoD Directive 1400.13 (reference (g)).

E2.1.12. DoD-Operated or -Sponsored Activity. A contracted entity authorized by appropriate DoD officials to perform child care, education, treatment, or

supervisory functions on DoD-controlled property (references (e), (g), (h), and (i)). Examples include but are not limited to CDPs, FCC Programs, Medical Treatment Facilities, DoDDS, DoD Section 6 Schools, and Youth Programs.

E2.1.13. DoD Section 6 Schools. The educational arrangements made for the provision of education to eligible dependent children by the Department of Defense under Pub. L. 81-874, Section 6, as defined in DoD Directive 1342.16 (reference (h)), in the Continental United States, Alaska, Hawaii, Puerto Rico, Wake Island, Guam, American Samoa, the Northern Mariana Islands, and the Virgin Islands.

E2.1.14. Family Child Care (FCC). Quarters-based child care provided in Government-owned or -leased quarters, in which care is provided on a regular basis for compensation, usually for more than 10 hours a week per child, to one or more (up to six) children, including the provider's own children under 8 years of age, as defined in reference (e).

E2.1.15. Foreign National Employees Overseas. Non-U.S. citizens hired by the Department of Defense for employment on an overseas installation.

E2.1.16. Foster Care. A voluntary or court-mandated program that provides 24-hour care and supportive services in a family home or group facility for children who cannot be properly cared for by their own family.

E2.1.17. Government-Contracted Care Providers. An individual or a group of individuals hired under a Government contract to provide instruction, child care services, healthcare, or youth services. FCC providers are not considered contracted Government employees for this Instruction.

E2.1.18. Healthcare Personnel. Personnel involved in the delivery of healthcare to children under the age of 18 on a frequent and regular basis. See enclosure 5. This may include:

E2.1.18.1. Medical and Dental Care Staff. Physicians, dentists, nurse practitioners, clinical social workers, clinical psychologists, physicians' assistants, physical therapists, and speech pathologists.

E2.1.18.2. Clinical Support Staff. Clinical providers not granted defined clinical privileges to include residents, registered nurses, licensed practical nurses, nursing assistants, play therapists, and technicians, as defined in DoD Directive 6025.11 (reference (i)).

E2.1.19. Installation Records Check (IRC). An investigation conducted through the records of all installations of an individual's identified residencies for the preceding 2 years before the date of the application. This record check shall include, at a minimum, police (base and/or military police, security office, or criminal investigators or local law enforcement) local files check, Drug and Alcohol Program, Family Housing, Medical Treatment Facility for Family Advocacy Program to include Service Central Registry records and mental health records, and any other record checks as appropriate, to the extent permitted by law.

E2.1.20. National Agency Check (NAC). As defined in DoD 5200.2-R (reference (c)).

E2.1.21. National Agency Check and Inquiries (NACI). As defined in the FPM, Chapters 731 and 736 (reference (b)).

E2.1.22. Nonappropriated Fund Instrumentalities (NAFI) Employees. Personnel hired by the DoD Components, compensated from NAFI funds as defined in DoD Directive 1015.1 (reference (j)). This includes temporary employees, 18 years old or older, who work with children.

E2.1.23. Private Organizations on DoD Installations. A nongovernmental entity authorized by the Department of Defense to perform child care, services, education, or supervisory functions with children on DoD-controlled property, as defined in DoD Instruction 1000.15 (reference (k)). Examples include religious groups and associations, such as scouts.

E2.1.24. Respite Care. Provides short-term child care and supportive services in a family home or group facility for children to relieve stress, prevent child abuse, and promote family unity for a parent, foster parent, guardian, or family member.

E2.1.25. Regular Contact. Responsible for a child or with access to children on a frequent basis as defined by the Component.

E2.1.26. Specified Volunteer Position. A position, designated by the DoD Component Head or designee, such as installation commander, requiring an installation record check because of the nature of the volunteer work in child care services.

E2.1.27. State Criminal History Repository (SCHR). The State's central record of investigative files. State information, including addresses, phone numbers, costs and remarks, is listed in enclosure 8.

E2.1.28. Supervision. Refers to having temporary responsibility for children in child care services, and temporary or permanent authority to exercise direction and control by an individual over an individual whose required background checks have been initiated but not completed.

E2.1.29. Temporary Employees. This category includes nonstatus appointments to a competitive service position for a specified period, not to exceed a year. This includes summer hires, student interns, and NAFI flexible category employees.

E2.1.30. Volunteer Activities. Activities where individuals offer assistance on an unpaid basis in child and youth programs or other activities on DoD installations. Examples include sports programs, religious programs, scouting programs, and preschools sponsored by private parent cooperatives or other associations conducted on the installation.

E2.1.31. Volunteers. Individuals who offer program assistance on an unpaid basis.

E2.1.32. Youth Programs. DoD-sponsored activities, events, services, opportunities, information, and individual assistance responsive to the recreational, developmental, social, psychological, and cultural needs of eligible children and youth. Includes before and after school programs as well as holiday and summer camps.

E3. ENCLOSURE 3

PUBLIC LAW 101-647, SECTION 231

LAWS OF 101st CONG.—2nd SESS.

Nov. 29

CRIME CONTROL ACT OF 1990

P.L. 101-647  
Sec. 231

**Subtitle E—Child Care Worker Employee  
Background Checks**

42 USC 13041.

**SEC. 231. REQUIREMENT FOR BACKGROUND CHECKS.**

(a) **IN GENERAL.**—(1) Each agency of the Federal Government, and every facility operated by the Federal Government (or operated under contract with the Federal Government), that hires (or contracts for hire) individuals involved with the provision to children under the age of 18 of child care services shall assure that all existing and newly-hired employees undergo a criminal history background check. All existing staff shall receive such checks not later than 6 months after the date of enactment of this chapter, and no additional staff shall be hired without a check having been completed.

(2) For the purposes of this section, the term "child care services" means child protective services (including the investigation of child abuse and neglect reports), social services, health and mental health care, child (day) care, education (whether or not directly involved in teaching), foster care, residential care, recreational or rehabilitative programs, and detention, correctional, or treatment services.

(b) **CRIMINAL HISTORY CHECK.**—(1) A background check required by subsection (a) shall be—

(A) based on a set of the employee's fingerprints obtained by a law enforcement officer and on other identifying information;

(B) conducted through the Identification Division of the Federal Bureau of Investigation and through the State criminal history repositories of all States that an employee or prospective employee lists as current and former residences in an employment application; and

(C) initiated through the personnel programs of the applicable Federal agencies.

(2) The results of the background check shall be communicated to the employing agency.

(c) **APPLICABLE CRIMINAL HISTORIES.**—Any conviction for a sex crime, an offense involving a child victim, or a drug felony, may be ground for denying employment or for dismissal of an employee in any of the positions listed in subsection (a)(2). In the case of an incident in which an individual has been charged with one of those offenses, when the charge has not yet been disposed of, an employer may suspend an employee from having any contact with children while on the job until the case is resolved. Conviction of a crime other than a sex crime may be considered if it bears on an individual's fitness to have responsibility for the safety and well-being of children.



(d) **EMPLOYMENT APPLICATIONS.**—(1) Employment applications for individuals who are seeking work for an agency of the Federal Government, or for a facility or program operated by (or through contract with) the Federal Government, in any of the positions listed in subsection (a)(1), shall contain a question asking whether the individual has ever been arrested for or charged with a crime involving a child, and if so requiring a description of the disposition of the arrest or charge. An application shall state that it is being signed under penalty of perjury, with the applicable Federal punishment for perjury stated on the application.

(2) A Federal agency seeking a criminal history record check shall first obtain the signature of the employee or prospective employee indicating that the employee or prospective employee has been notified of the employer's obligation to require a record check as a condition of employment and the employee's right to obtain a copy of the criminal history report made available to the employing Federal agency and the right to challenge the accuracy and completeness of any information contained in the report.

(e) **ENCOURAGEMENT OF VOLUNTARY CRIMINAL HISTORY CHECKS FOR OTHERS WHO MAY HAVE CONTACT WITH CHILDREN.**—Federal agencies and facilities are encouraged to submit identifying information for criminal history checks on volunteers working in any of the positions listed in subsection (a) and on adult household members in places where child care or foster care services are being provided in a home.

104 STAT. 4809

E4. ENCLOSURE 4

PUBLIC LAW 102-190, SECTION 1094

NATIONAL DEFENSE AUTHORIZATION ACT  
FOR FISCAL YEARS 1992 AND 1993

105 STAT. 1488

PUBLIC LAW 102-190—DEC. 5, 1991

**SEC. 1094. PROVISIONAL SUPERVISED EMPLOYMENT OF FEDERAL CHILD CARE SERVICES PERSONNEL.**

(a) **EMPLOYMENT PENDING COMPLETION OF BACKGROUND CHECK.**—Section 231 of the Crime Control Act of 1990 (42 U.S.C. 13041) is amended—

(1) in the second sentence of subsection (a)(1), by striking out “6 months after the date of enactment of this chapter, and no additional staff” and inserting in lieu thereof “May 29, 1991. Except as provided in subsection (b)(3), no additional staff”; and

(2) in subsection (b), by adding at the end the following new paragraph:

“(3) An agency or facility described in subsection (a)(1) may hire a staff person provisionally prior to the completion of a background check if, at all times prior to receipt of the background check during which children are in the care of the person, the person is within the sight and under the supervision of a staff person with respect to whom a background check has been completed.”.

(b) **ADDITIONAL SAFETY MEASURES FOR FEDERAL CHILD CARE SERVICE FACILITIES.**—It is the sense of Congress that each agency of the Federal Government, each facility operated by the Federal Government, and each facility operated under contract with the Federal Government, that provides child care services to children under the age of 18—

(1) modify child care facilities to the extent necessary to ensure that, except for restrooms, there are no secluded areas not open to the general view of persons in such facilities;

(2) provide for regular oversight of the management and operations of child care facilities by an agency official who is not directly in charge of the operation of the facility; and

(3) to the maximum extent feasible allow parental access to children in child care facilities at all times.

E5. ENCLOSURE 5

MEMORANDUM FROM THE SECRETARY OF DEFENSE HEALTH AFFAIRS,  
"CRIMINAL HISTORY BACKGROUND CHECKS ON HEALTHCARE  
PERSONNEL"



HEALTH AFFAIRS

THE ASSISTANT SECRETARY OF DEFENSE  
WASHINGTON, D. C. 20301-1200

APR 28 1992

MEMORANDUM FOR SECRETARY OF THE ARMY  
SECRETARY OF THE NAVY  
SECRETARY OF THE AIR FORCE

SUBJECT: Criminal History Background Checks on Child Health  
Care Personnel

This memorandum clarifies procedures for Department of Defense (DoD) health care personnel relative to implementation of Public Law 101-647, Section 231, "Crime Control Act," November 29, 1990, as amended by section 1094 of Public Law 102-190.

These provisions were implemented within DoD by Assistant Secretary of Defense (Force Management & Personnel) (ASD(FM&P)) memorandum, dated March 6, 1992, Subject: "Criminal History Background Checks on Employees in Child Care Services" (copy attached). The ASD(FM&P) memorandum requires Federal Bureau of Investigation (FBI) fingerprint checks and State Criminal History Repositories (SCHR) checks of residences listed on employment applications for specific existing and newly hired health care personnel. Active duty military members are excluded from the requirements of the statutory provisions and the ASD(FM&P) memorandum. As explained in the ASD(FM&P) memorandum, health care personnel are defined as:

"Those personnel involved in the delivery of health care to children under the age of 18 on a frequent and regular basis. This may include: (1) Medical and Dental Care Staff: physicians, dentists, nurse practitioners, clinical social workers, clinical psychologists, physician assistants, physical therapists, and speech pathologists. (2) Clinical Support Staff: clinical providers not granted defined clinical privileges to include residents, registered nurses licensed practical nurses, nursing assistants, play therapists, and technicians."

Two provisions of the ASD(FM&P) memorandum, when applied to the medical setting, require additional Health Affairs guidance.

1. The ASD(FM&P) memorandum states that:

"DoD components may employ an individual pending completion of successful background checks. If an individual is so employed, at all times while children are in the care of that individual, he or she must be within sight and under the supervision of an individual whose background checks have been completed, with no derogatory reports."

Processing reports can take months. It is unlikely that Congress meant to create a situation that would potentially require two physicians to examine a patient or two nurses to give one medication to a child.

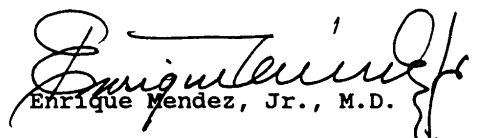
The DoD vigorously supports screening of health care workers involved in the delivery of health care to children under the age of 18 on a frequent and regular basis. Within the context of such medical care, line of sight supervision must be viewed through the prism of existing Medical Quality Assurance, Clinical Privileging, and Licensure Directives, which require pre-employment screens, enhanced surveillance of new employees and on-going monitoring of the performance of all health care providers. These programs are inherent to both quality medical care and patient safety and are adequate and equivalent mechanisms.

Therefore, pending completion of background checks, the Surgeons General shall require close clinical supervision and full compliance with existing DoD Directives, Instructions, and other guidance (issued by DoD and the Military Department concerned) on quality assurance, risk management, licensure, employee orientation, and credentials verification. These policies rely on process and judgment, and meet the intent of the "direct sight supervision" provision, affording local commanders a flexible and reasonable alternative.

2. Section 1094(b) of Public Law 102-190 provides that:

"It is the sense of Congress that each facility that provides childcare services to children under the age of 18 must modify child care facilities to the extent necessary that except for restrooms, there are no secluded areas not open to the general view of persons in such facilities."

This provision, which may be suitable for child development centers, is hortatory, not mandatory. Thus, the DoD must determine what effect to give it. Open areas in full view of the public eliminate patient privacy and, in some cases, are medically contraindicated. Thus, hospital commanders are not required to implement section 1094(b).

  
Enrique Mendez, Jr., M.D.

Attachment  
As Stated

## E6. ENCLOSURE 6

### CRIMINAL HISTORY BACKGROUND CHECK PROCEDURES

This enclosure establishes the procedures for conducting criminal history background checks on existing and newly hired individuals required by Pub. L. No. 101-647, Section 231 and Pub. L. No. 102-190, Section 1094 (enclosures 3 and 4). Background checks are required for all civilian providers involved in child care services who have regular contact with children. The categories of providers include current and prospective individuals hired with APF and NAFI funds for education, treatment or healthcare, child care or youth activities, and individuals employed under contract involved in the provision of child care services. In addition to the mandates of enclosure 3, the Department of Defense requires that military members (except healthcare personnel), foster or respite care providers, FCC providers and family members, and specified volunteers shall have checks specified in sections E6.1. through E6.10. of this enclosure, below.

#### E6.1. Conducting Checks

Component designees shall notify existing and newly hired individuals and contractors of the requirement for a review of personnel and security records to include an FBI fingerprint check and SCHR checks of residences listed on employment and security applications.

E6.1.1. Fingerprint Check. Law enforcement personnel shall forward completed forms through channels to the Office of Personnel Management (OPM) or Defense Investigative Service (DIS) for processing of FBI fingerprint forms.

E6.1.2. State Criminal History Repository (SCHR) Check. DoD Installation-level personnel offices, in collaboration with law enforcement and security personnel, shall process State criminal history background checks for employment and shall ordinarily communicate in writing with each State identified in enclosure 8, providing full identifying information on each applicant and request confirmation that the individual has not been convicted in that State of a sex crime, an offense involving a child victim, a drug felony, or a violent crime. The DoD Component Heads may establish alternate procedures for conducting SCHR checks; e.g., a computerized, written, or telephonic check. The DoD Components are not required to wait longer

than 60 days from the date of the request for a response from the SCHR personnel before taking action on a particular application. Authorities will depend on FBI fingerprint check validation if States do not respond.

E6.1.3. Installation Record Checks (IRC). Consists of a local record check on an individual for a minimum of 2 years before the date of the application. This record check shall include, at a minimum, police (base and/or military police, security office, criminal investigators, or local law enforcement) local files checks, Drug and Alcohol Program, Family Housing, Medical Treatment Facility for Family Advocacy Program Service Central Registry records and mental health records, and any other record checks as appropriate to the extent permitted by law. A Service DCII may be conducted. The IRC shall be conducted by DoD Component personnel at the installation level. An IRC will be completed on individuals with a DoD affiliation such as living or working on an installation or is active duty member or family member. Individuals without DoD affiliation have no installation system of records to check and an IRC is not completed. Upon favorable completion of the IRC, an individual may be selected and provide child care services under line of sight supervision until the required background checks are completed.

## E6.2. Applicants

### E6.2.1. APF Applicants

E6.2.1.1. Except as otherwise provided in this subsection, the DoD Components shall process APF applicants using currently established procedures for completing background checks described in DoD 5400.11-R (reference (a)). APF applicants must complete a SF-171, "Application for Federal Employment," and attach a SF-87, "Fingerprint Chart," completed by a law enforcement officer; and a SF-85P, "Questionnaire for Public Trust Positions" (Annotate Block "B" with code 03), for conduct of a NACI. The package shall be forwarded to the OPM.

E6.2.1.2. The DoD Components shall assign responsibility for conducting the criminal history background checks through the SCHR to personnel offices working with law enforcement or investigative agencies. They shall conduct checks in all States that an employee or prospective employee lists as current and former residences in an employment or security application. It is deemed unnecessary to conduct checks before 18 years of age because juvenile records are unavailable. If no response is received from the State(s) within 60 days, determinations based upon the FBI report may be made. Responses received after this determination has been made must be provided to the determining authority.

E6.2.1.3. Under Pub. L. No. 102-190, Section 1094 (enclosure 4), the DoD Components may employ an individual pending completion of successful background checks described in Pub. L. No. 101-647, Section 231 (enclosure 3). If an individual is so employed, at all times while children are in the care of that individual, he or she must be within sight and under the supervision of an individual whose background checks have been completed, with no derogatory reports.

E6.2.1.4. Once it is clear that no derogatory information exists, line of sight supervision is terminated by the designee. If a derogatory report exists, Component personnel procedures shall prescribe appropriate action consistent with the criteria contained in this Instruction.

#### E6.2.2. NAFI Applicants

E6.2.2.1. Except as otherwise provided in this subsection, the DoD Components shall process NAFI applicants following established procedures for completing background checks. NAFI applicants must complete a DD Form 398-2 "Department of Defense National Agency Questionnaire," with reason for request identified as OTHER and annotated as CHILD CARE, and FD Form 258, "FBI Applicant Fingerprint Card." Fingerprints shall be taken by the local law enforcement organization personnel and together with the DD Form 398-2 shall be forwarded to: Defense Investigative Service, Personnel Investigations Center, P.O. Box 1083, Baltimore, MD 21203-1083.

E6.2.2.2. The DoD Components shall follow the procedures in the FPM, Chapter 731 and 736 (reference (b)) and above in subparagraphs E6.2.1.2., E6.2.1.3., and E6.2.1.4. to obtain fingerprints for the FBI, conduct criminal history background checks through the SCHR, and maintain employment of individuals pending the successful completion of the background checks.

E6.2.3. Foreign National Employees Overseas. Foreign national employees overseas, while not expressly included within the law, are subject to the following record checks or those equivalent in scope to checks conducted on U.S. citizens:

E6.2.3.1. Host-government law enforcement and security agency checks at the city, State (province), and national level, whenever permissible by the laws of the host government.

E6.2.3.2. Defense Central Investigative Index (DCII).

E6.2.3.3. FBI checks (when information exists regarding residence by the individual in the United States for 1 year or more since age 18).

E6.2.3.4. When permissible by the laws of the host government, host-government checks are requested directly by the employing Service or agency. As an alternative, the DoD Components may request that overseas Military Service investigative elements obtain appropriate host-government checks. Where host-nations' arrangements preclude comparable criminal history checks, foreign nationals will not be eligible for employment in child care services.

E6.2.4. Temporary Employees. This category includes summer hires, student interns, and NAFI flexible category employees. Background checks for these individuals are processed according to funding source; i.e., for APF employees (to OPM) or NAFI employees (to DIS). Installation-designated points of contact shall notify applicants of report disposition.

E6.2.5. Healthcare Personnel. This category includes civilian personnel involved in the delivery of healthcare (enclosure 5). Within the context of such medical care, line of sight supervision must be viewed through the prism of existing medical quality assurance, clinical privileging, and licensure directives, which require preemployment screens, enhanced surveillance of new employees, and on going monitoring of the performance of all healthcare providers. These programs are inherent to both quality medical care and patient safety and are adequate and equivalent mechanisms for the sight and supervision requirements in paragraphs E6.2.1.3. and E6.2.1.4. of this enclosure, above. It should be noted that these quality assurance programs are not sufficient in and of themselves under Pub. L. No. 101-647, Section 231 (enclosure 3). Therefore, the required FBI fingerprint check and the SCHR check must be completed as expeditiously as possible.

### E6.3. Current Employees

All currently employed individuals covered by this Instruction shall have the FBI fingerprint and criminal history background check as described in Pub. L. No. 101-647, Section 231 (enclosure 3). If the results of such checks, to include the SCHR, cannot be confirmed through an examination of available local records, action shall be initiated in accordance with subsection E6.2.1., above, for APF employees and subsection E6.2.2., above, for NAFI employees, and with section E6.4., below, for individuals employed under contract. The SCHR checks are conducted in all cases in accordance with subsection E6.1.2., above. For the purposes of this Instruction, no



IRC is required for individuals employed before June 1991.

#### E6.4. Government Contract Employees

E6.4.1. Sponsoring activities are responsible for ensuring that the requirements in this Instruction are included in the statement of work for all child care programs to be contracted. The contracting officer is responsible for performing an action necessary to verify that services provided by the contractor conform to contract quality requirements. Component designees for requiring activities shall ensure that the statement of work, at a minimum:

E6.4.1.1. States that the contractor must ensure its employees have proper criminal history background checks as outlined in this Instruction.

E6.4.1.2. States that actual checks are performed by the Government.

E6.4.1.3. Includes procedures that the contractor must follow to obtain checks for its employees; for example, identify the office where employees report for processing, identify proper forms to be completed, etc. Also, identify the DoD Component for billing purposes, and identify the appropriate security point of contact or installation commander as the authorized recipient of background check results.

E6.4.1.4. States that employees may be permitted to work before completion of background checks, provided the employee is within sight of an individual who has successfully completed a background check.

E6.4.1.5. States that employees have the right to obtain a copy of the background check report, whom they should contact for the copy and whom to contact for procedures to challenge the accuracy and completeness of the information in the report.

E6.4.1.6. Requires that contractor employees who have previously received a background check must provide proof of the check or obtain a new one.

E6.4.2. Requirements for child care services must be submitted to the contracting officer sufficiently in advance of the required performance start date to provide time for obtaining background checks. Sponsoring activities' designees shall coordinate with the contracting officer as soon as possible after a requirement for child care services becomes known.

E6.4.3. Procedures for obtaining responses for background checks are the same as those for NAFI employees and response to derogatory information will occur through the appropriate designee and contractor. An IRC will be performed if the individual is a military member or family member, or has worked or lived on a military installation within 5 years.

#### E6.5. Other Providers

Criminal history background checks with the FBI and the States are not required. Duplication of previous background checks are not required for personnel where official records demonstrate that an adequate check has already been conducted. This category includes the following:

E6.5.1. Military Members. These are active duty individuals (other than healthcare personnel) who seek to provide child care services as part of a normal duty assignment or are involved during off-duty hours. For these members an IRC and a current security clearance meet the requirements of this Instruction. In the absence of a current security clearance, a name check of the DCII must be conducted. When military members are employed in an APF or a NAFI position they will abide by background check requirements listed in subsections E6.2.1. and E6.2.2., above.

E6.5.2. Foster and Respite Care Providers and Family Members. These are individuals who seek to provide foster care or respite child care within Government-owned or -leased quarters. The care provider, all other adults, and each child, age 12 and older, residing within the applicant's household must receive an IRC. In addition, the Component designee must also obtain a name check of the DCII on all adults.

E6.5.3. FCC Providers and Family Members. These are individuals who seek licensing to provide child care within Government-owned or -leased quarters. The care provider, all other adults, and each child, age 12 and older, residing within the applicant's household receive an IRC. In addition, the Component designee must obtain a name check of the DCII on all adults.

E6.5.4. Specified Volunteers. Installation commanders shall designate those positions that are determined to be "specified." Individuals working in specified volunteer positions will have an IRC check because of the nature of their work in child care services. The opportunity for contact may be extensive, frequent, or over a period of time. They include, but are not limited to, positions involving extensive

interaction alone, extended travel, and/or overnight activities with children. An IRC is required for volunteers who are active-duty, a family member, or a DoD civilian overseas. A volunteer is allowed to work upon completion of a favorable IRC. Background checks are not required for volunteers whose services will be of shorter duration than is required to perform the background checks and who are under line of sight supervision by an individual who has successfully completed a background check. The Components are required to provide additional implementing guidance.

#### E6.6. Employment Application Requirement

Pub. L. No. 101-647, Section 231 (enclosure 3) requires that each application for employment shall include a question asking whether the individual has ever been arrested for or charged with a crime involving a child, and, if so, requires a description of the disposition of the arrest or charge. The forms identified above in paragraphs E6.2.1.1. and E6.2.2.1. are signed by the applicant under penalty of perjury, with the applicable Federal punishment for perjury stated on the respective forms.

E6.6.1. An applicant's signature indicates an understanding of the employer's obligation to require a record check as a condition of employment. Information on background checks shall be maintained in accordance with applicable Component implementing regulations.

E6.6.2. Payment for the conduct of any criminal history background check is the responsibility of the requesting Service or Agency.

E6.6.3. The results of the background check are forwarded to the Component designee at the sending installation for appropriate action. A derogatory report would include, but not be limited to, the following applicable crimes: any charge or conviction for a sex crime, an offense involving a child victim, a substance abuse felony, or a violent crime.

E6.6.4. The hiring authority or designee is responsible for notifying the individual of a derogatory report. The individual may obtain a copy of the criminal history report and has the right to challenge the accuracy and completeness of any information contained in the report through the Privacy Program described in DoD 5400.11-R (reference (a)). The individual may provide information concerning positive mitigating factors for any adverse information presented.

E6.6.5. Employees whose criminal history background checks result in nonselection for employment or service shall be informed by the Component designee

of the right to an administrative appeal under reference (a). Under that Regulation, the individual may appeal with a specific request such as amendments to the records or request to file statement disagreeing with information in the record. If the employee's request for record information is refused, the individual is informed of his or her right to an administrative appeal. As appropriate, Component designees shall inform individuals of other avenues available to resolve matters of concern such as an administrative or negotiated grievance procedures. If the employee remains dissatisfied, he or she may seek a review. The Department of Defense recognizes the privacy interests and rights of all applicants and employees, and its own responsibility in ensuring a safe and secure environment for children within DoD activities or private organizations on DoD installations.

#### E6.7. Record Re-Verification

This procedure consists of an IRC and a DCII name check and is required by the Component designee at a minimum every 5 years for all employees providing child care services and covers the time period since the completion of the last background check. NAFI employees who change duty stations will complete a new investigation when considered for employment. A new investigation is required by the Department of Defense if a break in service results in a time-lapse of more than 2 years. FCC, foster care and respite care providers, and their family members will complete an IRC annually.

#### E6.8. Supervision

Refers to temporary responsibility for children in child care services, and relates to oversight for temporary or permanent authority to exercise direction and control by an individual over an individual whose required background checks have been initiated but not completed. Use of video equipment is acceptable provided it is monitored by an individual who has successfully completed a background check. Supervision procedures pending completion of background checks for healthcare personnel suggest that the Surgeons General shall require close clinical supervision and full compliance with existing DoD Directives, Instructions, and other guidance (issued by the Department of Defense and the Military Department concerned) on quality assurance, risk management, licensure, employee orientation, and credentials certification. These policies rely on process and judgment, and meet the intent of the "direct sight supervision" provision, affording local commanders a flexible and reasonable alternative.

## E6.9. Programs

Requirements cover all DoD-operated activities and private organizations on DoD installations and include, but are not limited to:

### E6.9.1. Child Development Programs.

E6.9.1.1. Child development centers, part-day preschools, and enrichment programs.

E6.9.1.3. Family child care.

E6.9.1.3. Contracted Services, whether personal or non-personal services.

### E6.9.2. Youth Programs.

E6.9.3. Dependents Schools operated by the Department of Defense.

E6.9.4. Medical treatment facilities.

E6.9.5. Other contracted services.

E6.9.6. Private organizations on DoD installations.

E6.9.7. Volunteer activities.

## E6.10. Background Check Matrix

This identifies the requirements of this Instruction for background checks by category of personnel. These checks are initiated through the personnel offices in collaboration with law enforcement and security personnel. (Reminder: An IRC may only be completed on an individual who is a military member or family member, or who lives or works on a military installation.)

E6.10.1. APF. FBI, SCHR, and IRC. (SF-171, SF-87, and SF-85P)

E6.10.2. NAFI. FBI, SCHR, and IRC. (DD Form 398-2 and FD Form 258)

E6.10.3. Foreign National Employees Overseas. IRC and local government check.

E6.10.4. Temporary Employees. FBI, SCHR, and IRC.

E6.10.5. Current Employees. FBI and SCHR.

E6.10.6. Government Contract Employees. FBI, SCHR, and IRC.

E6.10.7. Other Providers.

E6.10.7.1. Military Members. Military members will have an IRC and, if no current security clearance exists, a name check of the DCII. Checks are not required for military healthcare personnel.

E6.10.7.2. Foster and Respite Care Providers and Family Members (age 12 and older). IRC and Service DCII (for adults).

E6.10.7.3. FCC Providers and Family Members (age 12 and older). IRC and Service DCII (for adults).

E6.10.7.4. Specified Volunteers. IRC.

## E7. ENCLOSURE 7

### CRITERIA FOR CRIMINAL HISTORY BACKGROUND CHECK DISQUALIFICATION

The ultimate decision to determine how to use information obtained from the criminal history background checks in selection for positions involving the care, treatment, supervision, or education of children must incorporate a common sense decision based upon all known facts. Adverse information is evaluated by the DoD Component Head or designee who is qualified at the appropriate level of command in interpreting criminal history background checks. All information of record both favorable and unfavorable will be assessed in terms of its relevance, recentness, and seriousness. Likewise, positive mitigating factors should be considered. Final suitability decisions shall be made by that commander or designee. Criteria that will result in disqualification of an applicant require careful screening of the data and include, but are not limited to, the following:

#### E7.1. Mandatory Disqualifying Criteria

Any conviction for a sexual offense, a drug felony, a violent crime, or a criminal offense involving a child or children.

#### E7.2. Discretionary Criteria

E7.2.1. Acts that may tend to indicate poor judgment, unreliability, or untrustworthiness in working with children.

E7.2.2. Any behavior; illness; or mental, physical, or emotional condition that in the opinion of a competent medical authority may cause a defect in judgment or reliability.

E7.2.3. Offenses involving assault, battery, or other abuse of a victim, regardless of age of the victim.

E7.2.4. Evidence or documentation of substance abuse dependency.

E7.2.5. Illegal or improper use, possession, or addiction to any controlled or

psychoactive substances, narcotic, cannibas, or other dangerous drug.

E7.2.6. Sexual acts, conduct, or behavior that, because of the circumstances in which they occur, may indicate untrustworthiness, unreliability, lack of judgment, or irresponsibility in working with children.

E7.2.7. A wide range of offenses such as arson, homicide, robbery, fraud, or any offense involving possession or use of a firearm.

E7.2.8. Evidence that the individual is a fugitive from justice.

E7.2.9. Evidence that the individual is an illegal alien who is not entitled to accept gainful employment for a position.

E7.2.10. A finding of negligence in a mishap causing death or serious injury to a child or dependent person entrusted to their care.

### E7.3. Suitability Considerations

In making a determination of suitability, the evaluator shall consider the following additional factors to the extent that these examples are considered pertinent to the individual case:

E7.3.1. The kind of position for which the individual is applying or employed.

E7.3.2. The nature and seriousness of the conduct.

E7.3.3. The recentness of the conduct.

E7.3.4. The age of the individual at the time of the conduct.

E7.3.5. The circumstances surrounding the conduct.

E7.3.6. Contributing social or environmental conditions.

E7.3.7. The absence or presence of rehabilitation or efforts toward rehabilitation.

E7.3.8. The nexus of the arrests in regard to the job to be performed.

### E7.4. Questions



E7.4.1. All applications, for each of the categories of individuals identified in enclosure 2, will include the following questions: "Have you ever been arrested for or charged with a crime involving a child? Have you ever been asked to resign because of or been decertified for a sexual offense?" And, if so, "provide a description of the case disposition." For FCC, foster care, and respite care providers, this question is asked of the applicant regarding all adults, and all children 12 years and older, who reside in the household.

E7.4.2. All applications shall state that the form is being signed under penalty of perjury. In addition, a false statement rendered by an employee may result in adverse action up to and including removal from Federal service.

E7.4.3. Evaluation of criminal history background checks is made and monitored by qualified personnel at the appropriate level designated by the Component. Final suitability decisions are made by the designee.

E8. ENCLOSURE 8  
STATE INFORMATION

E8.1.1. All SCHR checks should be accompanied by the following:

E8.1.1.1. State form, if required. If no State form is required, the request should be on letterhead, beginning with the statement that the check is in accordance with Pub. L. No. 101-647 (enclosure 3). The request must include full identifying information, such as: Name, date of birth, social security number, complete addresses, etc.

E8.1.1.2. Fingerprint set if required. Some State laws require a fingerprint set either on a State form or forms used by the Agency.

E8.1.1.3. Release statement signed by the applicant or employee. If required by the State, the release must be notarized.

E8.1.1.4. Payment for the SCHR check.

E8.1.1.5. Self-addressed, stamped envelope.

E8.1.1.6. The following is an updated listing of State addresses, fees, and other information:

ADDRESS	FEE	REMARKS
State of Alabama Alabama Dept. of Public Safety ATTN: ABI Division 5002 Washington Ave. Montgomery, AL 36130	\$25	Name check  COMM: 205-242-4372
State of Alaska Alaska Dept. of Public Safety Information Systems Section 5700 Tudor Road Anchorage, AK 99507	\$20	Fingerprints req'd, reason for request req'd (comply with Pub. L.), Name and Address authorized to request and receive SCHRC COMM: 907-269-5 511

ADDRESS	FEE	REMARKS
State of Arizona Arizona Criminal Justice Dept. of Public Safety Information Systems Division P.O. Box 6638 Phoenix, AZ 85005	No Check	Limited release, call or write for information.  COMM: 602-223-2229
State of Arkansas Arkansas State Police P.O. Box 5901 Little Rock, AR 72215	No Fee	Name Check Written Consent Req'd  COMM: 501-221-8233
State of California Dept. of Justice Bureau of Criminal Justice Identification and Information Bureau P.O. Box 903417 Sacramento, CA 94203-4170	\$27	Fingerprints Req'd  COMM: 916-739-2786
State of Colorado Crime Information Center Colorado Bureau of Investigation 690 Kipling Street, #3000 Lakewood, CO 80215	\$ 4.50	Write or call for form Name Check  COMM: 303-239-4222/4229
State of Connecticut Dept. of State Police Bureau of Investigation, Building 4 294 Colony Street Meriden, CT 06450	No Fee	Name Check Written Consent Req'd Copy of Pub. L. Req'd COMM: 203-238-6155
State of Delaware Delaware State Police-SBI State Bureau of Investigation P.O. Box 430 Dover, DE 19903	\$25	Fingerprints Req'd  COMM: 302-739-5871
Washington, DC Identification and Records Division Metropolitan Police Dept., Room 2076 300 Indiana Avenue, N.W. Washington, DC 20001	No Fee	Name Check Written Request Req'd COMM: 202-727-4245
State of Florida Florida Dept. of Law Enforcement P.O. Box 1489 Tallahassee, FL 32302	\$10	Name Check Check to: Dept. of Law Enforcement COMM: 904-488-6236

ADDRESS	FEE	REMARKS
State of Georgia Georgia Criminal Information Center Post Office Box 370748 Decatur, GA 30037-0748	\$15	Write or call for form Notary & Fingerprints Req'd COMM: 404-244-2644
State of Hawaii Criminal Justice Data Center 465 South King Street, Room 101 Honolulu, HI 96813	No Fee	Name Check  COMM: 808-587-3100
State of Idaho Idaho Dept. of Law Enforcement Criminal Identification Bureau 6064 Corporal Lane Boise, ID 83704	\$5	Name Check Written Consent Req'd Payment to: Dept. of Law Enforcement COMM: 208-327-7130
State of Illinois Bureau of Identification 260 North Chicago Street Joliet, IL 60431-1060	\$14	Write or call for form Name Check COMM: 815-740-5184
State of Indiana Indiana State Police 100 North Senate Avenue, Room 312 Indianapolis, IN 46204	\$7	Write or call for form Name Check COMM: 317-232-8266
State of Iowa Commissioner Paul H. Wieck II Iowa Dept. of Public Safety Wallace State Office Building Des Moines, IA 50319	\$6	Release within State  COMM: 515-281-5138
State of Kansas Kansas Bureau of Investigation 1620 Southwest Tyler Topeka, KS 66612	\$10	Write or call for form Name Check, \$5 per name over two names COMM: 913-232-6000
State of Kentucky Kentucky State Police Records State Office Building 1250 Louisville Road Frankfort, KY 40601	\$4	Write or call for form Name Check  COMM: 502-227-8700 x214

ADDRESS	FEES	REMARKS
State of Louisiana Louisiana State Police Department of Public Safety P.O. Box 66614 Baton Rouge, LA 70896	\$13	Write or call for form Fingerprints Req'd  COMM: 504-925-6095
State of Maine State Bureau of Identification Department of Public Safety Maine State Police, 36 Hospital Street Augusta, ME 04333	No Fee	Name Check Reason for Check Req'd, i.e., Comply with Pub. L. COMM: 207-624-7009
State of Maryland Criminal Justice Information Service Central Repository, Building G4 1201 Reistertown Road Pikesville, MD 21208	\$18	Write or call for form Name Check  COMM: 410-764-4501
State of Massachusetts Executive Office of Public Safety Criminal History Systems Board 1010 Commonwealth Avenue Boston, MA 02215	No Fee	Write or call for form Name Check COMM: 617-727-0090 x12
State of Michigan Michigan State Police, FOI Unit 7150 Harris Drive Lansing, MI 48913	No Check	No release  COMM: 517-322-5531
State of Minnesota Criminal Justice Information Systems Bureau of Criminal Apprehension Minnesota Dept. of Public Safety 1246 University Avenue St. Paul, MN 55104	\$8	Name Check Written Consent Req'd COMM: 612-642-0670
State of Mississippi Department of Public Safety ATTN: Identification Bureau P.O. Box 958 Jackson, MS 39225	No Fee	Write or call for info Name Check  COMM: 601-987-1212
State of Missouri Criminal Records Division State Highway Patrol Department of Public Safety P.O. Box 568 Jefferson City, MO 65102	\$5	Write or call for form Name Check  COMM: 314-751-3313

ADDRESS	FEES	REMARKS
State of Montana Identification Bureau Department of Justice 303 North Roberts Helena, MT 59620-1418	\$5	Name Check  COMM: 406-444-3625
State of Nebraska Nebraska State Patrol P.O. Box 94907 State House Station, ATTN: CID Lincoln, NE 68509-4907	\$10	Name Check  COMM: 402-471-4545
State of Nevada Nevada Highway Patrol 555 Wright Way Carson City, NV 89711	\$15	Write or call for form Fingerprints Req' d  COMM: 702-687-5300
State of New Hampshire New Hampshire State Police HQ Criminal Records 10 Hazen Drive Concord, NH 03305	\$10	Write or call for form Name Check  COMM: 603-271-2538
State of New Jersey Division of State Police Records and ID Section P.O. Box 7068 West Trenton, NJ 08625-0068	\$12	Copy of Pub. L. Req'd Name Check  COMM: 609-882-2000
State of New Mexico Department of Public Safety Records Bureau P.O. Box 1628 Santa Fe, NM 87504-1628	\$5	Write or call for form Name Check, Notary Req'd COMM: 505-827-9181
State of New York Division of Criminal Justice Services Executive Park Tower Stuyvesant Plaza Albany, NY 12203	No Check	No Release at current time, State Req's an Agreement with Agency to process. COMM: 518-485-7685
State of North Carolina Division of Criminal Information Bureau of Investigation 407 North Blount Street Raleigh, NC 27601-1009	\$14	Fingerprint form req'd, Copy of Pub. L. req'd, Call or write for form COMM: 919-662-4500

ADDRESS	FEES	REMARKS
State of North Dakota Bureau of Criminal Information P.O. Box 1054 Bismark, ND 58502	\$20	Name Check Written Consent Req'd COMM: 701-221-6180
State of Ohio Bureau of Criminal Information P.O. Box 365 London, OH 43140	\$15	Write or call for form Written Consent Req'd Fingerprints Req'd COMM: 614-852-2556
State of Oklahoma Oklahoma Law Enforcement Criminal History Information ATTN: Criminal History P.O. Box 11497 Oklahoma City, OK 73136	\$10	Write or call for form Name Check  COMM: 405-848-6724
State of Oregon Criminal ID, State Police 155 Cottage Street, NE Salem, OR 97310	\$10	Name Check  COMM: 503-378-3070
State of Pennsylvania Records and ID Division Pennsylvania State Police, Dept. HQ 1800 Elmerton Avenue Harrisburg, PA 17110	\$10	Write or call for form Name Check COMM: 717-783-5592
State of Rhode Island Rhode Island State Police P.O. Box 185 North Scituate, RI 02857	No Fee	Name Check Written Consent Req's  COMM: 401-647-3311
State of South Carolina State Law Enforcement Division ATTN: Criminal Records Post Office Box 21398 Columbia, SC 29221-1398	\$10	Name Check  COMM: 803-737-4205 DSN: 734-1110
State of South Dakota Division of Criminal Investigation Attorney General's Office East Highway 34 Pierre, SD 57501-5070	\$15	Write or call for form Fingerprints Req'd COMM: 605-773-3331

ADDRESS	FEES	REMARKS
State of Tennessee Tennessee Crime Information Center Tennessee Bureau of Investigation P.O. Box 100940 Nashville, TN 37210	\$23	Write or call for form Fingerprints Req'd COMM: 615-741-3241
State of Texas Texas Crime Records Division Texas Dept. of Public Safety P.O. Box 15999 Austin, TX 78761-5999	\$15	Fingerprints Req'd Written Consent Req'd COMM: 512-465-2079
State of Utah Bureau of Criminal Identification Utah Dept. of Public Safety 4501 South 2700 West Salt Lake City, UT 84119	No Fee	Write or call for form Name Check Copy of Law Req'd COMM: 801-965-4571
State of Vermont Vermont Criminal Information Center Dept. of Public Safety P.O. Box 189 Waterbury, VT 05676	No Fee	Name Check Written Consent Req'd  Comm: 802-244-8786
Commonwealth of Virginia Virginia Records Management Division Dept. of State Police P.O. Box 850761 Richmond, VA 23261-5076	\$10	Write or call for form Name Check  COMM: 804-674-2024
State of Washington Washington State Patrol Identification Section P.O. Box 42633 Olympia, WA 98504-2633	\$10	Write or call for form Name Check  COMM: 206-753-0230/7272
West Virginia State Police Dept. of Public Safety 725 Jefferson Road South Charleston, WV 25309	\$5	Write or call for form Name Check COMM: 304-746-2180
State of Wisconsin Crime Information Bureau Dept. of Justice ATTN: Records Data Unit P.O. Box 2718 Madison, WI 53701-2718	\$2	Write or call for form Name Check COMM: 608-266-7314



ADDRESS	FEES	REMARKS
State of Wyoming Division of Criminal Investigation 316 West 22nd Street Cheyenne, WY 82002	\$15	Write or call for form Fingerprints Req'd Written Consent Req'd COMM: 307-777-7181



# Department of Defense INSTRUCTION

NUMBER 6490.06

April 21, 2009

*Incorporating Change 1, July 21, 2011*

---

---

USD(P&R)

SUBJECT: Counseling Services for DoD Military, Guard and Reserve, Certain Affiliated Personnel, and Their Family Members

References: See Enclosure 1

1. PURPOSE. This Instruction establishes and implements counseling policies and identifies and assigns responsibilities for providing counseling support in accordance with the authority in DoD Directive (DoDD) 5124.02 (Reference (a)).

2. APPLICABILITY. This Instruction applies to:

a. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to as the "DoD Components"). The term "Military Services" as used herein refers to the Army, the Navy, the Air Force, and the Marine Corps.

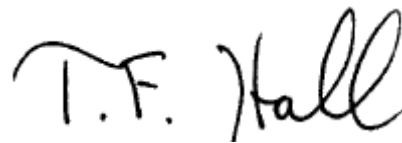
b. Members of the Active Component and of the Army National Guard, Army Reserve, Air National Guard, Air Force Reserve, Marine Corp Reserve, and Naval Reserve (hereafter referred to as the "Active and Reserve Components") *and* their family members ~~and, when authorized by the Secretary of the Military Department, DoD civilian employees and their family members.~~

*c. DoD civilian personnel designated as Civilian Expeditionary Workforce members pursuant to DoDD 1404.10 (Reference (b)) and their family members.*

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy to:

- a. Promote a culture that encourages delivery and receipt of counseling.
  - b. Eliminate barriers to and the negative stigma associated with seeking counseling support.
  - c. Empower leaders to advocate for those in their charge to receive counseling.
  - d. Provide easy access to a continuum of counseling support to include prevention, early intervention, and treatment to enhance coping and build resilience.
  - e. View counseling support as a force multiplier enhancing military and family readiness.
5. RESPONSIBILITIES. See Enclosure 2.
  6. PROCEDURES. See Enclosure 3.
  7. RELEASABILITY. UNLIMITED. This Instruction is approved for public release and is available on the Internet from the DoD Issuances Website at <http://www.dtic.mil/whs/directives>.
  8. EFFECTIVE DATE. This Instruction is effective immediately.



T. F. Hall  
Performing the Duties of the  
Under Secretary of Defense  
for Personnel and Readiness

Enclosures

1. References
2. Responsibilities
3. Procedures

Glossary

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 5124.02, "Under Secretary of Defense for Personnel and Readiness (USD(P&R))," June 23, 2008
- (b) *DoD Directive 1404.10, "DoD Civilian Expeditionary Workforce," January 23, 2009*
- (~~bc~~) DoD Instruction 6400.06, "Domestic Abuse Involving DoD Military and Certain Affiliated Personnel," August 21, 2007
- (~~ed~~) DoD Directive 6495.01, "Sexual Assault Prevention and Response (SAPR) Program," October 6, 2005
- (~~de~~) Section 552a of title 5, United States Code
- (~~ef~~) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
- (~~fg~~) DoD ~~Directive~~*Instruction* 6025.18, "Privacy of Individually Identifiable Health Information in DoD Health Care Programs," ~~December 19, 2002~~*December 2, 2009*
- (~~gh~~) American Psychiatric Association, "Diagnostic and Statistical Manual of Mental Disorders, Fourth Edition (DSM-IV)," 1994
- (~~hi~~) DoD Instruction 1342.27, "Personnel Financial Management for Service Members," November 12, 2004
- (~~ij~~) DoD Instruction 1342.22, "Family Centers," December 30, 1992
- (~~jk~~) Public Law 110-289, "Housing and Economic Recovery Act of 2008," July 30, 2008
- (~~kl~~) Sections 501-596 of title 50, United States Code
- (~~lm~~) Chapter 55 and sections 836 and 1145 of title 10, United States Code
- (~~mn~~) DoD Directive 6400.1, "Family Advocacy Program (FAP)," August 23, 2004
- (~~no~~) DoD Instruction 6495.02, "Sexual Assault Prevention and Response Program Procedures," June 23, 2006

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS (USD(P&R)). The USD(P&R) shall:

a. Develop and maintain this Instruction and ensure DoD Component compliance with its policies.

b. Collaborate with the Military Departments to establish procedures and programs consistent with this Instruction.

c. Program, budget, and allocate funds and other resources to meet the policy objectives of this Instruction.

d. Ensure that information on military and civilian mental health research and programs is exchanged among the Department of Defense and the Military Services.

2. DEPUTY ~~UNDER ASSISTANT~~ SECRETARY OF DEFENSE FOR MILITARY COMMUNITY AND FAMILY POLICY (~~DUSD-DASD~~(MC&FP)). The ~~DUSD~~ ~~DASD~~(MC&FP), under the authority, direction, and control of the USD(P&R), shall:

a. Provide through Military OneSource (MOS) and the Military and Family Life Consultant (MFLC) Program, non-medical, brief counseling support to augment counseling provided by the Active and Reserve Components.

b. Provide, through MOS and the MFLC Program, personal financial counselors to augment personal financial planning and counseling provided by the Active force and Reserve Components.

c. Provide guidance and technical assistance to the DoD Components in addressing counseling initiatives.

d. Collaborate with the DoD Components and Federal and State agencies that address counseling; serve on related Federal committees and advisory groups.

e. Promote general awareness of counseling programs among the DoD Components.

f. Monitor compliance with this Instruction and periodically evaluate DoD counseling programs in collaboration with the organizations mentioned in this Instruction.

3. ASSISTANT SECRETARY OF DEFENSE FOR RESERVE AFFAIRS (ASD(RA)). The ASD(RA), under the authority, direction, and control of the USD(P&R), shall collaborate with the Military Departments and the USD(P&R) to establish procedures and programs consistent with this Instruction.

4. SECRETARIES OF THE MILITARY DEPARTMENTS. The Secretaries of the Military Departments shall:

a. Establish policies and programs consistent with the procedures outlined in section 6 of Enclosure 3 and ensure implementation, monitoring, and evaluation at all levels of military command.

b. Program, budget, and allocate funds and other resources to meet the policy objectives of this Instruction.

c. Provide annual education and training to key personnel on the policies and procedures in this Instruction.

d. Ensure leadership oversight at all levels of implementation.

ENCLOSURE 3

PROCEDURES

1. MOS AND MFLC PROGRAMS. MOS and MFLC Program counselors provide non-medical, short-term, solution-focused counseling and briefings for circumstances amenable to brief intervention, including but not limited to stress and anger management, grief and loss, the deployment cycle, parent-child relationships, couples communication, marital issues, relationships, and relocations based on the needs of the community being served. The counseling approach is psycho-educational, which helps participants learn to anticipate and resolve challenges associated with the military lifestyle. This non-medical support is aimed at preventing the development or exacerbation of mental health conditions that may detract from military and family readiness.

a. MOS and MFLC Programs shall implement privacy and confidentiality policies to promote participation and reduce stigma, except to meet legal obligations or to prevent harm to self or others.

(1) Information disclosed to MOS and MFLC Program counselors shall be kept confidential, except to meet legal obligations or to prevent harm to self or others. (See Glossary for definitions of “legal obligation” and “harm to self or others.”)

(2) MOS and MFLC Program counselors are not authorized to receive a domestic abuse or sexual assault restricted report. If the person receiving counseling requests restricted reporting pursuant to domestic abuse or sexual assault, the MOS and MFLC Program counselors shall transfer the person to a specified individual who is authorized to receive a restricted report in the respective Military Service according to DoD Instruction (*DoDI*) 6400.06 (Reference (*bc*)) and DoDD 6495.01 (Reference (*ed*)).

(3) At a minimum, any personally identifiable information recorded by MOS and MFLC Program counselors is subject to section 552a of title 5, United States Code (U.S.C.) (Reference (*de*), commonly referred to as the “Privacy Act of 1974”) and DoD 5400.11-R (Reference (*ef*)); however, because MOS and the MFLC Program are not healthcare programs, this information may not be subject to DoD ~~DI~~ 6025.18 (Reference (*fg*)).

(4) At a minimum, this confidentiality statement shall be provided to all eligible individuals seeking counseling services pursuant to this Instruction: “Information you provide to me or other counselors will be kept confidential, except to meet legal obligations or to prevent harm to self or others. Legal obligations include requirements of law and DoD or military regulations. Harm to self or others includes suicidal thought or intent, a desire to harm oneself, domestic violence, child abuse or neglect, violence against any person, and any present or future illegal activity.”

b. MOS and MFLC Program counselors do not provide clinical therapy. Situations requiring clinical therapy such as those meeting the diagnostic criteria found in American Psychiatric

Association Manual (Reference (~~g~~*h*)) shall be referred to a military medical treatment facility, TRICARE, or other providers of professional mental healthcare.

c. MOS and MFLC Program counselors providing direct non-medical counseling support shall have at least a Masters degree from an accredited graduate program in a mental health-related field such as social work, psychology, marriage and family therapy, or counseling; a valid unrestricted counseling license or certification from a State, the District of Columbia, a U.S. Commonwealth, or a U.S. Territory that grants authority to provide counseling services as an independent practitioner in their respective fields; and demonstrated current counseling competence preceding their employment with MOS or the MFLC program.

d. MOS services are provided face-to-face (continental United States (CONUS) only) to individuals, couples, families, and groups, and telephonically or over the Internet to individuals worldwide. MOS services may be accessed 24 hours a day, 7 days a week using the toll free number 1-800-342-9647 or on the Internet at <http://www.militaryonesource.com>. Eligible participants may receive twelve non-medical counseling sessions per person per issue.

(1) Face-to-face non-medical counseling is provided using a nationwide network of affiliate providers who have been screened by MOS to assure they meet the requirements of paragraph 1.c. of this enclosure.

(2) In addition to non-medical counseling support, MOS provides personalized assistance with special-needs family members, child care, relocation, health and wellness, translation services, and more.

e. The MFLC Program provides worldwide non-medical counseling support in accordance with these service delivery options:

(1) Rotational. Rotational non-medical counseling support in which MFLC Program counselors travel to designated areas to provide temporary support is available to the active force in and outside CONUS to augment counseling services provided by the Military Departments. Service delivery may occur on or off military installations. Non-medical counseling is provided face-to-face, to individuals, couples, families, and groups. Rotations may not exceed 90 days. Requests for rotational support must be submitted through the appropriate designated Military Service headquarters points of contact to the Office of the ~~DUSD~~*DASD*(MC&FP).

(2) On-Demand. On-demand non-medical counseling support is provided to the Reserve Components for mobilization, deployment, and reunion activities. Units and commands may request on-demand support by completing a request form at <http://jfsap.mhf.dod.mil/request>. Requests are submitted through the appropriate Reserve Component chain of command to the Office of the ~~DUSD~~*DASD*(MC&FP). On-demand support may also be requested by calling toll free 1-888-256-9920.

(3) Full-Time. MFLC Programs may provide full time non-medical counseling support for special projects such as legislatively or DoD-mandated programs.



f. Additional information on the MFLC program may be found at <http://www.militaryhomefront.dod.mil/service/counseling>.

2. PERSONAL FINANCIAL COUNSELING. Personal financial counselors assist with issues including, but not limited to, developing saving and investing strategies, spending plans, understanding military benefits, purchasing a home, debt management, taxes, and financial emergencies. Circumstances requiring legal assistance shall be referred accordingly. Financial counselors shall operate in accordance with DoD/~~Instruction~~ 1342.27 (Reference (~~h~~)).

a. Personal financial management is a baseline service in all DoD family centers (DoD/~~Instruction~~ 1342.22 (Reference (~~i~~))).

b. MOS financial counselors are available face-to-face or by phone at 1-800-342-9647.

c. MFLC Program financial counselors provide face-to-face support in accordance with the rotational and on-demand service delivery options contained in paragraphs 1.e.(1) and 1.e.(2) of this enclosure and may be requested using procedures contained in those paragraphs.

d. Members of the Active force and Reserve Components may utilize the State and Territory Transition Assistance Advisors to access information about local financial counseling resources.

e. Service members covered by this Instruction who are returning from and departing for service on active duty abroad shall be advised on actions to take to prevent or forestall mortgage foreclosures including, but not limited to, credit counseling, home mortgage counseling, and such other counseling and information appropriate for this purpose (Public Law 110-289 (Reference (~~j~~))). They will also be provided, in writing, notice about the appropriate provisions of sections 501-596 of title 50, U.S.C. (Reference (~~k~~)), commonly known as the “Servicemember’s Civil Relief Act”). All members covered by this Instruction shall be advised on actions to forestall mortgage foreclosures in accordance with section 1 of this enclosure.

3. FAMILY CENTERS. Reference (~~i~~) governs family centers.

a. Family centers provide baseline services and may, without releasing DoD Components of their obligations to perform functions required by statute or DoD policy, provide other support programs including but not limited to non-medical counseling for individuals, couples, and families.

b. Family center staff providing non-medical counseling shall meet the criteria in paragraph 1.c. of this enclosure and criteria established by the respective Military Departments.

c. Contact information for DoD family centers may be found at <http://www.militaryinstallations.dod.mil>.

4. CHAPLAINS. Authorized personnel counseled by military chaplains in a manner intended to be confidential, and made either as a formal act of religion or as a matter of conscience, shall be entitled to the protections of privileged communication as delineated under military rules of evidence (section 836 of title 10, U.S.C. (Reference (~~lm~~))), applicable statutes, regulations, and service policies. Chaplains may provide counseling to individuals, couples, families, and groups. Authorized personnel may request chaplain counseling services through direct contact or via appropriate Service protocols.

5. FAMILY ADVOCACY PROGRAM (FAP). DoD Directive 6400.1 (Reference (~~mn~~)) governs the FAP.

a. FAP addresses family violence in military families through prevention, early identification, and intervention.

b. FAP provides support for victims and treatment for abusers, to include clinical therapy, marital therapy, and support groups.

c. Contact information for DoD FAPs may be found at <http://www.militaryinstallations.dod.mil>.

6. MILITARY HEALTH SYSTEM (MHS). The MHS ensures delivery of world-class healthcare to all DoD Service members, retirees, and their families. The MHS provides non-medical counseling and clinical therapy at military medical treatment facilities (MTFs) and through TRICARE.

a. MTFs are the primary source of specialty mental healthcare for military personnel. Services may include clinical therapy for mental health conditions, such as post traumatic stress disorder, major depression, and conditions found in Reference (~~gh~~). They also provide non-medical counseling for issues related to work, school, or family.

b. Active duty Service members seeking mental healthcare through the TRICARE network must obtain a referral from their military medical support office or their primary care provider.

c. Dependents may receive up to eight outpatient non-medical or clinical therapy treatment sessions per year from a TRICARE network mental healthcare provider without prior authorization. The mental healthcare provider must seek authorization from the TRICARE contractor for additional visits.

d. Reserve Component members and their families may also be eligible for non-medical counseling and clinical therapy through TRICARE in accordance with chapter 55 and section 1145 of Reference (~~lm~~).

e. The MHS mental health provider shall provide a copy of the Military Health System Notice of Privacy Practices, available at <http://www.tricare.osd.mil/tmaprivacy>, to patients upon intake for their initial care.

7. SEXUAL ASSAULT PREVENTION AND RESPONSE (SAPR). Reference (~~ed~~) and DoDI ~~Instruction~~ 6495.02 (Reference (~~no~~)) govern sexual assault prevention and response.

a. SAPR allows for care and services to be delivered to victims of sexual assault. Service member victims may make either a restricted report or an unrestricted report and may receive treatment and services pursuant to Reference (~~no~~).

b. Only individuals specified in Reference (~~ed~~) may receive restricted reports.

c. Additional information about DoD and Military Service SAPR policies may be obtained at <http://www.sapr.mil> or by calling the Sexual Assault Prevention and Response Office at 703-696-9422.

## GLOSSARY

### DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purpose of this Instruction.

child abuse. Defined in Reference (~~mn~~).

clinical therapy. Therapy provided for circumstances amenable to long-term therapeutic intervention by a clinical provider. Clinical therapy may be provided to individuals, couples, and families. Issues such as post traumatic stress disorder, depression, traumatic brain injury, drug and alcohol abuse, child and spouse abuse, suicidal ideation, or conditions meeting the diagnostic criteria found in Reference (~~gh~~) may be addressed in clinical therapy. This definition is not intended to limit the authority of the Military Departments to grant privileges to clinical providers modifying this scope of care consistent with current Military Department policy.

domestic abuse. Defined in Reference (~~bc~~).

family center. Defined in Reference (~~ij~~).

family member. Defined in Reference (~~ij~~).

FAP. Defined in Reference (~~mn~~).

financial planning and counseling. Defined in Reference (~~hi~~).

harm to others. Includes circumstances indicating a danger of domestic violence, child abuse or neglect; violence against any person; or present or other future illegal activity.

harm to self. Includes circumstances indicating suicidal thought, intent, or a desire to harm oneself. For Service members this includes any expression of past or present illegal use of controlled substances while on active duty.

legal obligations. Uses and disclosures of information that are required by Federal law, applicable State law, applicable host-nation law outside the United States, or DoD or Military Service regulations and similar issuances.

non-medical counseling. Short term, non-therapeutic counseling that is not appropriate for individuals needing clinical therapy. Non-medical counseling is supportive in nature and addresses general conditions of living, life skills, improving relationships at home and at work, stress management, adjustment issues (such as those related to returning from a deployment), marital problems, parenting, and grief and loss. This definition is not intended to limit the authority of the Military Departments to grant privileges to clinical providers modifying this scope of care consistent with current Military Department policy.

psycho-education. A means to educate people through counseling, trainings, or activities addressing topics including but not limited to those listed in the definition of non-medical counseling in this Glossary. Psycho-education helps people learn to anticipate and resolve challenges, make informed decisions, communicate effectively, develop coping and self-management skills, and may help prevent the development or exacerbation of mental health conditions that may detract from military and family readiness.

restricted reporting

Defined in Reference (~~b~~*c*) as it applies to adult victims of domestic abuse who are eligible to receive military medical treatment, including civilians and contractors who are eligible to receive military healthcare outside CONUS on a reimbursable basis.

Defined in Reference (~~e~~*d*) as it applies to Service members who report or disclose being victims of sexual assault.

**ATTACHMENT – 21**  
**PERFORMANCE WORK STATEMENT (PWS)**  
**MONTHLY REPORTING REQUIREMENTS**  
**MILITARY ONESOURCE PROGRAM**

1. **REPORTING REQUIREMENTS.** The following specified documents are requirements of this PWS. Nothing in these documents, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

1.1. Program Report

- 1.1.1. Narrative executive summary of work accomplished during the reporting period.
- 1.1.2. Problem areas or issues that have been identified during the period and resolution action taken, if any.
- 1.1.3. Attached to this report will be copies of any reports (informal and formal) that have been provided to any DoD organization during the period. Individual Military Service Branch and installation reports will be prepared and submitted monthly as attachments to the monthly contracting report.
- 1.1.4. Utilization information for the current month, percent change since the same month of the previous fiscal year, utilization for the current fiscal year to date, and percent change from fiscal year to date of the previous year, in the following categories.
- 1.1.5. Overall Utilization / Key Metrics
  - 1.1.5.1. Incoming phone contacts
  - 1.1.5.2. Outgoing phone contacts
  - 1.1.5.3. Client Call Back Statistics
  - 1.1.5.4. Cases by email
  - 1.1.5.5. Email contacts
  - 1.1.5.6. Top five reasons to call, go online
- 1.1.6. Counseling
  - 1.1.6.1. Referrals to in-person counseling
  - 1.1.6.2. In-person counseling sessions conducted
  - 1.1.6.3. Referrals to STSF telephonic counseling sessions
  - 1.1.6.4. STSF telephonic counseling sessions conducted
  - 1.1.6.5. Requests for web-based counseling
  - 1.1.6.6. Web-based counseling sessions conducted
  - 1.1.6.7. In-person financial counseling sessions conducted
  - 1.1.6.8. Telephonic financial counseling sessions conducted
  - 1.1.6.9. Requests for healthy habits coaching
  - 1.1.6.10. Online coaching sessions conducted
  - 1.1.6.11. Telephonic coaching sessions conducted
  - 1.1.6.12. Duty status and rank of counseling participants,
  - 1.1.6.13. Average number of counseling sessions provider per client
  - 1.1.6.14. Average distance of network provider from client residence
  - 1.1.6.15. Referrals to Military Treatment Facility
  - 1.1.6.16. Referrals to Red Cross
  - 1.1.6.17. Referrals to Tricare

**ATTACHMENT – 21**  
**PERFORMANCE WORK STATEMENT (PWS)**  
**MONTHLY REPORTING REQUIREMENTS**  
**MILITARY ONESOURCE PROGRAM**

- 1.1.6.18. Total referrals to Family Advocacy Program
- 1.1.6.19. Total referrals to Sexual Assault Response Coordinator
- 1.1.6.20. Total referrals to Victim Advocacy
- 1.1.6.21. Top five reasons for: STSF counseling, financial counseling
- 1.1.6.22. Contractor will report summary on each Duty to Warn case to include Military Branch and a brief narrative of the situation requiring Duty to Warn.
- 1.1.6.23. Average number of sessions utilized for cases closed during reported month
- 1.1.6.24. Types of counseling provided: individual, group, family, couple
  - 1.1.6.24.1. Top 10 primary Client issues for non-medical counseling programs
  - 1.1.6.24.2. Top 3 primary provider/employee issues pertaining to NMCPs (pp)
  - 1.1.6.24.3. Top 5 referred-to providers for NMCPs (per program [pp])
  - 1.1.6.24.4. Top 5 components using NMCP services
- 1.1.7. Educational Materials
  - 1.1.7.1. Ordered through call center
  - 1.1.7.2. Ordered online
  - 1.1.7.3. Bulk ordered
- 1.1.8. Translation/Interpretation Services
  - 1.1.8.1. Documents translated
  - 1.1.8.2. Top 5 types of documents translated
  - 1.1.8.3. Interpretation Sessions/Month
  - 1.1.8.4. Type of Service Requiring Interpreter Services (i.e. Spouse Counseling, MOS Triage, Materials Request)
- 1.1.9. WWRC
  - 1.1.9.1. Cases
  - 1.1.9.2. New cases
  - 1.1.9.3. Cases resolved
  - 1.1.9.4. Cases outside of 96 hour compliance
  - 1.1.9.5. Calls
  - 1.1.9.6. Incoming calls transferred from MOS consultant
  - 1.1.9.7. Navy Safe Harbor calls
  - 1.1.9.8. Outbound calls
- 1.1.10. Child Care: number of referrals to Child Care Aware
- 1.1.11. Special Needs
  - 1.1.11.1. Number of calls
  - 1.1.11.2. Number of new cases
  - 1.1.11.3. Types of cases by issue (behavioral, physical, adult, child, etc.)
- 1.1.12. JFSAP
  - 1.1.12.1. Events supported by type
    - 1.1.12.1.1 Events supported by location (State or Territory)
    - 1.1.12.1.2 Events supported by location (City or Installation)
    - 1.1.12.1.3 Attendees at supported events by Branch and Component

**ATTACHMENT – 21**  
**PERFORMANCE WORK STATEMENT (PWS)**  
**MONTHLY REPORTING REQUIREMENTS**  
**MILITARY ONESOURCE PROGRAM**

- 1.1.12.2. Total number of Contact Types
  - 1.1.12.2.1 Briefing: Face to Face, Virtual
  - 1.1.12.2.2 Presentation: Face to Face, Virtual
  - 1.1.12.2.3 Community Capacity Building
    - 1.1.12.2.3.1 List of Organizations contacted for Outreach
      - 1.1.12.3.1.1 Total number of virtual sessions for organization
      - 1.1.12.3.1.2 Total number of emails to organization
      - 1.1.12.3.1.3 Total number of phone calls to organization
      - 1.1.12.3.1.4 Total number of Partnership Meetings with the organization
      - 1.1.12.3.1.5 Total number of Collaborative Meetings with the organization
- 1.1.12.4 Total number of Participants for each Contact listed above
- 1.1.12.5 Top 5 Reasons for Briefings
- 1.1.12.6 Top 5 Presentations
  - 1.1.12.6.1 By State
  - 1.1.12.6.2 By Branch of Service and Component
- 1.1.13. Spouse Education and Career Opportunities (SECO). MyCAA is a subset of SECO. The SECO program is to transition (not-to-exceed 90 days) to the new SECO provider.
  - 1.1.13.1. Number of calls to SECO (not MyCAA) and number of calls to SECO for MyCAA
  - 1.1.13.2. Average handling time per call for SECO (not MyCAA) and average handling time per call to SECO for MyCAA
  - 1.1.13.3 Date of oldest phone message to be returned for SECO (not MyCAA) and date of oldest phone message to be returned for MyCAA
  - 1.1.13.4 Total phone messages for SECO (not MyCAA) and total phone messages for MyCAA
  - 1.1.13.5 Number of MyCAA messages needing to be returned in BAM portal
  - 1.1.13.6 Date of oldest MyCAA message in BAM portal
  - 1.1.13.7. Number of spouses assisted in each of the following areas for SECO(not MyCAA eligible) and MyCAA eligible:
    - 1.1.13.7.1 Career Exploration
    - 1.1.13.7.2 Education and Training
    - 1.1.13.7.3 Career Readiness
    - 1.1.13.7.4 Career Connections
  - 1.1.13.8 Number of SECO specialty appointments in the following areas:
    - 1.1.13.8.1 Career Exploration
    - 1.1.13.8.2 Education and Training
    - 1.1.13.8.3 Career Readiness
    - 1.1.13.8.4 Career Connections
  - 1.1.13.9 Number of Referrals to the SECO Program (AFTER transition)



**ATTACHMENT – 21**  
**PERFORMANCE WORK STATEMENT (PWS)**  
**MONTHLY REPORTING REQUIREMENTS**  
**MILITARY ONESOURCE PROGRAM**

1.1.14. Tax

- 1.1.14.1. Number of calls
- 1.1.14.2. Number of Federal returns filed
- 1.1.14.3. Number of State returns filed
- 1.1.14.4. Total number of returns filed FYTD

1.1.15. Quality

- 1.1.15.1. QASP/QCP report including all metrics in QCP
  - 1.1.15.1.1. Customer recovery
    - 1.1.15.1.1.1. Complaints
    - 1.1.15.1.1.2. Complaints escalated
    - 1.1.15.1.1.3. Complaints resolved
  - 1.1.15.1.2. # of duty to warn notifications
    - 1.1.15.1.2.1. From call center
    - 1.1.15.1.2.2. From network
  - 1.1.15.1.3. # of warm handoffs
    - 1.1.15.1.3.1. From call center
    - 1.1.15.1.3.2. From network

1.1.16. Personnel and Training

- 1.1.16.1. Providers total in the network
- 1.1.16.2. Providers added to network
- 1.1.16.3. Providers trained
- 1.1.16.4. Providers left network
- 1.1.16.5. Providers ejected from network
- 1.1.16.6. Open and closed cases
- 1.1.16.7. Position management report
- 1.1.16.8. All positions in the contract filled, not filled, advertised, etc.

1.1.17. Communications and Strategic Outreach

- 1.1.17.1. Webinars conducted, topics, attendees
- 1.1.17.2. Moderated chats conducted, topics, attendees
- 1.1.17.3. Materials released
- 1.1.17.4. E-newsletters
- 1.1.17.5. Advertising efforts

1.2. Financial Disbursement Report

- 1.2.1. The Contract Fund Status Report will include the amount invoices to date, the amount received in payments to date, the amount that has been invoiced but not paid and the funds remaining not invoiced. All information will be reported by CLIN/Sub-CLIN.
- 1.2.2. Cumulative hours expended throughout the reporting period by job category