



United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

FEB 27 2017

PERSONNEL BULLETIN NO: 17-05

SUBJECT: Standardized Position Descriptions for Bureau Associate Chief Information Security Officers.

1. Purpose. This bulletin establishes Department of the Interior standard position descriptions (SPDs) for supervisory and non-supervisory Bureau Associate Chief Information Security Officers (ACISO) at the GS-15 level.

2. Background. The SPDs are part of the Department's implementation of the Federal Information Technology Acquisition Reform Act (FITARA), specifically supporting requirements related to the enhancement of hiring, performance management and workforce planning within information management and technology programs. The Department's Office of Human Resources (OHR) and Office of the Chief Information Officer (OCIO) collaborated to establish these SPDs. The OCIO vetted SPDs with bureau/office leadership through the Information Management and Technology Leadership Team (IMTLT) and Bureau Chief Information Security Officers (BCISOs). The OHR considered input from Bureau Classification Leads.

3. Policy. Bureau human resources offices should work with appropriate offices to ensure all ACISOs are on the appropriate SPD within six (6) months of issuance of this bulletin. The official SPDs with SPD numbers covered by this Personnel Bulletin are:

- Information Technology Specialist (Security), GS-2210-15 (SPD Number DOI005)
- Supervisory Information Technology Specialist (Security), GS-2210-15 (SPD Number DOI006)

In accordance with Personnel Bulletin 16-05, Servicing Human Resource Offices (SHRO) and the relevant Associate Chief Information Officer (ACIO) must ensure that the Department Chief Information Security Officer (CISO), or his/her designee, is involved in the recruitment and will approve the selection of the ACISO.

4. Position Titles:

Official Titles. In accordance with the law (5 U.S.C. 5105) the U.S. Office of Personnel Management (OPM) must establish official titles for positions based on the occupational series assigned. These prescribed titles are specified in published classification standards. Titles are based on their occupational series and any specialized function it performs (i.e., Information Technology Specialist). These titles must be coded into FPPS and be reflected on the

incumbent's SF-50, *Notification of Personnel Action*. The official titles assigned to the ACISO SPD follow the OPM standards for the GS-2210 series.


Organizational Titles. In addition to the official title, the agency has the option to assign an organizational title that reflects the position's organizational placement or specific program focus. For example, a position classified as a GS-2210-15 may have an official title of Supervisory Information Technology Specialist (or Supervisory IT Specialist) and an organizational title of Associate Chief Information Security Officer. The organizational title assigned to the above SPDs is **Associate Chief Information Security Officer**.

5. Standard PD Numbering System. Bureaus/Offices must implement the DOI SPD numbering system for newly established positions when replacing existing PDs with the SPDs. The DOI SPD number must be entered into FPPS, in accordance with Bureau procedures, so it prints on the incumbent's SF-50, *Notification of Personnel Action*. The SPD number is recorded in Block 1 of the OF-8 attached for each DOI SPD. In order to conform to the position number data field in FPPS, the SPD numbers assigned are seven digits in length.

6. Management's Responsibility for PD Accuracy and Position Management. Use of Standardized PDs in no way detracts from management's authority and responsibility to ensure that officially assigned and performed duties and responsibilities accurately match PDs of record for all covered employees. Likewise, using SPDs also does not diminish management's responsibility to adhere to basic position management principles. Management officials are urged to contact their respective servicing human resources office for classification and position management advice and guidance.

7. Exception to the Rules. Bureaus may make some updates to these SPDs to reflect bureau-specific requirements. However, major changes that will alter the classification and/or grades of the positions should be avoided. Bureau Human Resources Offices and Associate Chief Information Officers must fully coordinate any changes to these SPDs or establishment of lower graded position descriptions with the Department's Chief Information Security Officer and Office of Human Resources.

Questions concerning SPDs should be directed to the respective Bureau/equivalent Human Resources Office. The DOI, Office of Human Resources contact is Martin Pursley at martin_pursley@ios.doi.gov.



Raymond A. Limon
Director, Office of Human Resources

Attachments

OF 8, SPD #DOII005, IT Specialist (Security), GS-2210-15

OF 8, SPD #DOII006, Supervisory IT Specialist (Security), GS-2210-15

POSITION DESCRIPTION <i>(Please Read Instructions on the Back)</i>						1. Agency Position No. DOI1005	
2. Reason for Submission <input type="checkbox"/> Redescription <input checked="" type="checkbox"/> New <input type="checkbox"/> Reestablishment <input type="checkbox"/> Other Explanation <i>(Show any positions replaced)</i> Standard PD		3. Service <input type="checkbox"/> Hdqtrs <input checked="" type="checkbox"/> Field		4. Employing Office Location		5. Duty Station	
		7. Fair Labor Standards Act <input checked="" type="checkbox"/> Exempt <input type="checkbox"/> Nonexempt		8. Financial Statements Required <input type="checkbox"/> Executive Personnel Financial Disclosure <input type="checkbox"/> Employment and Financial Interest		9. Subject to IA Action <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
		10. Position Status <input checked="" type="checkbox"/> Competitive <input type="checkbox"/> Excepted <i>(Specify in Remarks)</i> <input type="checkbox"/> SES (Gen.) <input type="checkbox"/> SES (CR)		11. Position Is <input type="checkbox"/> Supervisory <input type="checkbox"/> Managerial <input checked="" type="checkbox"/> Neither		12. Sensitivity <input type="checkbox"/> 1--Non-Sensitive <input type="checkbox"/> 3--Critical <input type="checkbox"/> 2--Noncritical Sensitive <input checked="" type="checkbox"/> 4--Special Sensitive	
13. Competitive Level Code		14. Agency Use					
15. Classified/Graded by		Official Title of Position		Pay Plan	Occupational Code	Grade	Initials Date
a. Office of Personnel Management		Information Technology Specialist (Security)		GS	2210	15	
b. Department, Agency or Establishment							
c. Second Level Review							
d. First Level Review							
e. Recommended by Supervisor or Initiating Office							
16. Organizational Title of Position <i>(if different from official title)</i> Associate Chief Information Security Officer				17. Name of Employee <i>(if vacant, specify)</i>			
18. Department, Agency, or Establishment Department of the Interior				c. Third Subdivision			
a. First Subdivision Office of the Chief Information Officer				d. Fourth Subdivision			
b. Second Subdivision Bureau Associate Chief Information Officer				e. Fifth Subdivision			
19. Employee Review-This is an accurate description of the major duties and responsibilities of my position.				Signature of Employee <i>(optional)</i>			
20. Supervisory Certification. <i>I certify that this is an accurate statement of the major duties and responsibilities of this position and its organizational relationships, and that the position is necessary to carry out Government functions for which I am responsible. This certification is made with the knowledge that</i>				<i>this information is to be used for statutory purposes relating to appointment and payment of public funds, and that false or misleading statements may constitute violations of such statutes or their implementing regulations.</i>			
a. Typed Name and Title of Immediate Supervisor				b. Typed Name and Title of Higher-Level Supervisor or Manager <i>(optional)</i>			
Signature _____ Date _____				Signature _____ Date _____			
21. Classification/Job Grading Certification. <i>I certify that this position has been classified/graded as required by Title 5, U.S. Code, in conformance with standards published by the U.S. Office of Personnel Management or, if no published standards apply directly, consistently with the most applicable published standards.</i>				22. Position Classification Standards Used in Classifying/Grading Position			
Typed Name and Title of Official Taking Action Renae Lockwood, Sr. HR Specialist (Class/Comp)				OPM Job Family Standard for Administrative Work in the Information Technology Group, 2200, Issued May 2001, Revised August 2003, September 2008, and May 2011			
Signature <div style="display: flex; justify-content: space-between; align-items: flex-start;"> <div>RENAE LOCKWOOD</div> <div style="font-size: small;">Digitally signed by RENAE LOCKWOOD Date: 2017.02.10 07:37:42 -05'00'</div> </div>				Date 02/10/2017			
23. Position Review		Initials Date		Initials Date		Initials Date	
a. Employee <i>(optional)</i>							
b. Supervisor							
c. Classifier							
24. Remarks							
25. Description of Major Duties and Responsibilities <i>(See Attached)</i>							

Instructions for Completing Optional Form 8

POSITION DESCRIPTION

In order to comply with the requirements of FPM Chapter 295, subchapter 3, and other provisions of the FPM, agencies must complete the items marked by an asterisk. Agencies may determine what other items are to be used.

- *1. Enter position number used by the agency for control purposes. See FPM Chapter 312, Subchapter 3.
- *2. Check one.
 - "Redescription" means the duties and/or responsibilities of an existing position are being changed.
 - "New" means the position has not previously existed.
 - "Reestablishment" means the position previously existed, but had been cancelled.
 - "Other" covers such things as change in title or occupational series without a change in duties or responsibilities.
 - The "Explanation" section should be used to show the reason if "Other" is checked, as well as any position(s) replaced by position number, title, pay plan, occupational code, and grade.
- 3. Check one.
- *4. Enter geographical location by city and State (or if position is in a foreign country, by city and country).
- *5. Enter geographical location if different from that of #4.
- 6. To be completed by OPM when certifying positions. (See Item 15 for date of OPM certification.) For SES and GS-16/18 positions and equivalent, show the position number used on OPM Form 1390 (e.g., DAES0012).
- *7. Check one to show whether the incumbent is exempt or nonexempt from the minimum wage and overtime provisions of the Fair Labor Standards Act. See FPM Chapter 551.
- 8. Check box if statement is required. See FPM Chapter 734 for the Executive Personnel Financial Disclosure Report, SF 278. See FPM Chapter 735, Subchapter 4, for the Employment and Financial Interests Statement.
- 9. Check one to show whether identical additional positions are permitted. See FPM Chapter 312, Subchapter 4. Agencies may show the number of such positions authorized and/or established after the "Yes" block.
- 10. Check one. See FPM Chapter 212 for information on the competitive service and FPM Chapter 213 for the excepted service. For a position in the excepted service, enter authority for the exception, e.g., "Schedule A-213.3102(d)" for Attorney positions excepted under Schedule A of the Civil Service Regulations. SES (Gen) stands for a General position in the Senior Executive Service, and SES (CR) stands for a Career Reserved position.
- 11. Check one.
 - A "Supervisory" position is one that meets the requirements for a supervisory title as set forth in current OPM classification and job-grading guidance. Agencies may designate first-level supervisory positions by placing "1" or "1st" after "Supervisory."
 - A "Managerial" position is one that meets the requirements for such a designation as set forth in current OPM classification guidance.
- 12. Check one to show whether the position is non-sensitive, noncritical sensitive, critical sensitive, or special sensitive for security purposes. If this is an ADP position, write the letter "C" beside the sensitivity.

13. Enter competitive level code for use in reduction-in-force actions. See FPM Chapter 351.

14. Agencies may use this block for any additional coding requirement.

*15. Enter classification/job grading action.

- For "Official Title of Position," see the applicable classification or job grading standard. For positions not covered by a published standard, see the General Introduction to "Position Classification Standards," Section III, for GS positions, or FPM Supplement 512-1, "Job Grading System for Trades and Labor Occupations," Part 1, Section III.

- For "Pay Plan code, see FPM Supplement 292-1, "Personnel Data Standards," Book III.

- For "Occupational Code," see the applicable standard; or, where no standard has been published, see the "Handbook of Occupational Groups and Series of Classes" for GS positions, or FPM Supplement 512-1, Part 3, for trades and labor positions. **For all positions in scientific and engineering occupations, enter the two-digit functional classification code in parentheses immediately following the occupational code, e.g., "GS-1310(14)." The codes are listed and discussed in the General Introduction to "Position Classification Standards," Section VI.**

16. Enter the organizational, functional, or working title if it differs from the official title.

17. Enter the name of the incumbent. If there is no incumbent, enter "vacancy."

*18. Enter the organizational location of the position, starting with the name of the department or agency and working down from there.

19. If the position is occupied, have the incumbent read the attached description of duties and responsibilities. The employee's signature is optional.

*20. This statement normally should be certified by the immediate supervisor of the position. At its option, an agency may also have a higher-level supervisor or manager certify the statement.

*21. This statement should be certified by the agency official who makes the classification/job grading decision. Depending on agency regulations, this official may be a personnel office representative, or a manager or supervisor delegated classification/job grading authority.

22. Enter the position classification/job grading standard(s) used and the date of issuance, e.g., "Mail and File, GS-305, May 1977."

23. Agencies are encouraged to review periodically each established position to determine whether the position is still necessary and, if so, whether the position description is adequate and classification/job grading is proper. See FPM Letter 536-1 (to be incorporated into FPM Chapter 536). This section may be used as part of the review process. The employee's initials are optional. The initials by the supervisor and classifier represent recertifications of the statements in items #20 and #21 respectively.

24. This section may be used by the agency for additional coding requirements or for any appropriate remarks.

*25. Type the description on plain bond paper and attach to the form. The agency position number should be shown on the attachment. See appropriate instructions for format of the description and for any requirements for evaluation documentation, e.g., "Instructions for the Factor Evaluation System," in the General Introduction to "Position Classification Standards," Section VII.

Department of the Interior
Information Technology Specialist (Security)
Associate Chief Information Security Officer (ACISO)
GS-2210-15

I. Introduction

This is a standardized position description for the Department's Associate Chief Information Security Officers (ACISOs) located in the various Bureaus and Offices of the Department. The ACISO reports to the Bureau Associate Chief Information Officer (ACIO), and the Departmental Chief Information Security Officer (CISO) located in the Office of the Chief Information Officer (OCIO). The ACISO is accountable for collaboration on Departmental Information Technology (IT) Security policy and implementation of the Department's IT Security Program within their respective Bureau.

The ACISO serves as their assigned Bureau's senior subject matter expert and principal technical advisor and consultant to the ACIO, and is responsible for providing strategic leadership vision, direction, and coordination in support of Departmental IT Security Program activities across their assigned Bureau. This position is required for the protection of information and information systems and for providing a framework to manage and measure IT Security program performance, promote increased awareness throughout the Bureau, and to reduce potential breaches of sensitive Bureau information and the compromise of information systems.

II. Major Duties

IT Security Leadership: 25%

The ACISO serves as the senior subject matter expert, principal technical advisor, and consultant to the ACIO by providing strategic leadership vision, direction, and coordination in support of Departmental IT Security Program activities across the Bureau. The ACISO has primary responsibility on all matters pertaining to the security of information and information systems supporting Bureau assets including budget formulation and execution, security auditing, security awareness training, business security policy, and compliance reporting. The ACISO:

- Serves as principal Bureau liaison to the Department OCIO on all issues related to IT security.
- Manages an IT Security Office within the Bureau with the mission and resources necessary to ensure Departmental compliance with Section 3554 of FISMA.
- Provides expert guidance to senior agency officials concerning responsibilities under

paragraph 3554 (a) (2) of FISMA.

- Serves as lead advisor in network and systems design to ensure implementation of appropriate systems security policies, advises on developing system security contingency plans and disaster recovery procedures.
- Provides expert technical, analytical, and managerial guidance for the planning, review, evaluation, implementation, coordination, and integration of IT Security requirements within the Bureau's IT architecture.
- Promotes awareness of IT security issues among management and conducts security briefings and training to foster institutionalized awareness of the Bureau's Security Program and accepted security practices.
- Represents the Bureau on Federal government and industry committees, groups, and task forces concerned with security issues, policies, standards, guidance, and practices to address opportunities, challenges, or problems relating to IT and information management.
- Provides oversight to personnel with significant responsibilities for information security.

IT Security Policy Interpretation and Development: 25%

The ACISO has primary responsibility for the development of IT security policy within assigned Bureau that advances secure IT solutions and services residing on a reliable, secure, cost-efficient and effective supporting infrastructure. The ACISO exercises authority in the management, regulation, assessment, and reporting of Bureau IT security, and ongoing assessment for compliance with Department, Federal, and National Institute of Standards and Technology (NIST) policies, directives, guidelines, and best practices. The ACISO also has responsibility for reporting on the performance of the bureau-wide IT Security Program and the development of Bureau IT security policies and procedures. The ACISO:

- Directs development, develops, and maintains Bureau IT security policies, procedures, and guidance to ensure information systems confidentiality, integrity and availability, to prevent and defend against unauthorized access to systems, networks, and data systems, and to address all applicable requirements, including those issued under Section 3553 of FISMA, and Section 11331 of Title 40.
- Interprets Government-wide information security guidelines and establishes standards, policies, guidelines, and control techniques to ensure appropriate application, implementation, and compatibility of IT security on Bureau systems.
- Initiates, manages, coordinates, and assures maintenance of formal and informational documentation associated with the Bureau's IT Security Program.
- Establishes Bureau-wide IT Security education, awareness, and training for required employees and contractors.
- Collaborates with the Departmental CISO in development and/or revision of Department

IT security policies and procedures.

- Ensures communication of and timely compliance with all Department IT security policies, procedures, and directions.
- Coordinates all Bureau activities in response to IT Security policies, procedures and directions including development and implementation of operational IT security activities, collection of information, and submission of reports.
- Participates on Government-wide advisory boards along with other cabinet level agencies to draft Governmental IT Security policy, and make Government-wide IT security recommendations.

IT Security Operations 25%

The ACISO has primary responsibility for ensuring Bureau information systems confidentiality, integrity and availability, and the prevention and defense against unauthorized access to systems, networks, and data. The ACISO oversees, manages, and provides coordination, technical guidance, and direction on all aspects of the IT security operations within the Bureau including:

- Coordinates implementation of the Departmental IT Risk Management Framework, Assessment and Authorization, and associated enterprise-wide continuous monitoring processes, procedures and programs to reduce the risk of vulnerabilities and weaknesses that could adversely impact the confidentiality, integrity or availability of sensitive agency information and information systems.
- Provides oversight in the monitoring of all Bureau systems development and operations for IT security compliance.
- Conducts risk and vulnerability assessments of planned and installed information systems to identify vulnerabilities, risks, and protection needs for the Bureau.
- Provides oversight to ensure Bureau IT components are assessed and authorized to fully meet Federal computer security requirements.
- Oversees systems security evaluations, audits, and reviews.
- Directs an IT security operations program by providing management and direction over contractor support tasks and work orders, identifying funding, manpower, and technical requirements and descriptions of the work to be accomplished; planning and establishing work schedules, deadlines, and standards for acceptable work; coordinating and integrating contractor work schedules and processes with the work of others; tracking progress and quality of performance; and deciding on the acceptability, rejection, or correction of work products or services, and similar matters which may affect payment to the contractor.
- Leads or oversees evaluations of IT security activities, provides briefings and recommendations to management on major IT security problems or issues discovered during evaluations, and develops comprehensive reports of findings and remediation

actions.

- Maintains awareness of current developments in the area of IT security, information management and information technologies.
- Establishes and leads Computer Security Incident Response teams, and is the primary Bureau contact for all cybersecurity incidents.
- Maintains awareness of potential threats to the security and/or integrity of Bureau data; stays abreast of threat activity to include computer viruses, patterns and methods of unauthorized intrusion in other government computer systems; communicates effectively and in a timely manner with all staff organizations regarding potential threats; conducts security briefings and other types of security training to foster an awareness of the IT Security Program throughout the Bureau.
- Oversees IT Security Audit and Risk Programs, conducting periodic evaluations and reviews to ensure the effective implementation of security safeguards and that the Security Program is in compliance with existing directives and appropriate to the risks and sensitivity of each computer application.
- Oversees a security monitoring program to ensure that security safeguards implemented within an information system are not circumvented.

Team Leader Duties (25%)

Leads a variety of Bureau multi-disciplinary teams critical to the protection of Bureau and Departmental information assets. Responsibility at this level requires exceptional coordination and integration of a number of segments or programs of technical work that could be politically sensitive and cause legal ramifications if not implemented properly. Program responsibility involves major decisions and actions which have a direct and substantial effect on other organizations and programs in the Bureau and the Department. As Team Leader, plans and directs the work of the team, establish work priorities, assigns work, assesses performance and makes recommendations to supervisor. Incumbent provides technical guidance and plans work to be accomplished by team members, establishing priorities and scheduling work to meet suspense established by the ACIO. While this position performs team leader duties 25 percent of the time, the position does not lead a defined group of employees. Rather, the ACISO performs lead duties over teams that are project and/or matrix based.

Performs other related duties as assigned.

Condition of Employment

SPECIAL SENSITIVE (requiring Top Secret & SCI access) no waiver's allowed:

This position is designated as a SPECIAL SENSITIVE National Security position. Prior to appointment (Entrance on Duty), it requires a fully completed and favorably adjudicated

National Security Background Investigation (SSBI or SSBI-PR) that is current (within the last 5 years). Once employed, further processing for special access approval (SCI) will also occur.

III. Factor Levels

Factor 1 - Knowledge Required by the Position

Level 1-9 (1850 Points)

Mastery of IT theories, principles, concepts, standards, and practices sufficient to develop new theories, concepts, principles, standards and methods in security and to serve as senior expert and consultant to top Department and Bureau management officials to define issues and problems and to advise top information management executives concerning developments of integrating IT programs and solving the most complex technical problems.

Mastery of IT security theories and concepts, practices and emerging issues, and project management methods and concepts sufficient to plan and coordinate implementation of bureau-wide IT strategies consistent with government wide IT security defense strategies to ensure protection of the Bureau's IT infrastructure and to serve as Departmental Liaison.

Expert knowledge of and skill in applying information security principles, concepts, methods, standards and practices in order to provide strategic direction and leadership in the development and management of IT operating systems, applications, networks, and related equipment.

Expert knowledge of IT security issues, solutions, practices, concepts, trends, and capabilities relating to implementing policies and safeguards to protect information, networks, and systems.

Mastery of regulatory requirements and legislation including the Clinger-Cohen Act, FISMA, GPRA, OMB Circular A-130, OMB Circular A-11, etc., impacting Bureau IT network operations, objectives, and goals.

An exceptionally broad knowledge of IT, Web, and Telecommunications security policies, regulations, laws, standards, and procedures mandated internally or by oversight agencies.

Expert knowledge of state-of-the-art IT technology and current Federal IT management policies and principles concerning systems development, security and utilization of IT related equipment and software.

Comprehensive knowledge of Federal, Departmental, Bureau, and industry information security standards, principles and policies in order to plan, develop, and coordinate Bureau level information Security Programs and strategies.

Analysis and decision making skills sufficient to resolve complex security problems, analyze alternatives, recommend solutions, review/revise current Bureau security policies, and establish new policies.

Communication skills, both verbally and in writing, sufficient to present complex technical information to individuals (Bureau and Departmental management, staff, contractors, etc.) to facilitate constructive discussion, and to obtain consensus or agreement. Develops networks, builds alliances, and finds common ground with a broad range of stakeholders. Using non-traditional methodologies, collaborates with others in the administration of programs ensuring that stakeholder input is appropriately considered. Uses strategic thinking to develop innovative solutions and ensures conflicts are managed and/or resolved in a positive and constructive manner to maximize results.

Factor 2 - Supervisory Controls

Level 2-5 (650 Points)

The ACISO takes executive direction from the ACIO and the CISO who provide broad policy, program and administrative guidance. Incumbent works under broad delegated authority and has wide latitude to act independently within designated areas of responsibility to make judgments, decisions, and commitments based upon independent judgment and discretion.

The ACISO develops, plans, and executes the Bureau's IT security program, including approval, allocation, and distribution of funds. In addition, the ACISO has the authority to set multi-year strategic goals and schedules. The ACISO originates and/or initiates many assignments and has responsibility for forming and coordinating the work of a team, as required, to plan, design, and carry out studies, projects, and other work.

The ACISO is recognized as the Bureau's source of knowledge and resident subject matter expert on all IT security matters, and results of the work are considered technically authoritative and normally accepted without change. The employee's actions, decisions, and recommendations are reviewed primarily for results obtained in achieving security goals and objectives, and in providing support for the attainment of the organization's mission responsibilities. The supervisor evaluates the employee's recommendations for new or revised IT security policies, procedures, and controls in terms of impact on subject-matter program goals and objectives, and national IT security priorities. The incumbent keeps management informed of progress, potentially controversial matters, or far-reaching implications of the work.

Factor 3 - Guidelines

Level 3-5 (650 Points)

Guidelines are all applicable Federal and State laws, legislative histories of those laws, court decisions interpreting those laws, and agency regulations and directives, including Federal regulations, Departmental policies, National Institute of Standards and Technology (NIST) technical publications, and IT policies and standards. These guidelines are frequently nonspecific and stated in terms of broad national or Department policies and goals. The incumbent is a recognized technical authority and uses judgment and ingenuity and exercises broad latitude in determining the intent of the guidelines or combinations of the guidelines and how they apply in a given situation. The ACISO is responsible for developing new approaches

and solutions based upon applicable policies, regulations, or laws.

Guidelines also include technical and security briefings regarding system vulnerabilities and the incumbent must use swift and decisive action to interpret effects on the organization and initiate remediation activities. Due to rapidly evolving technology, some guidelines may be out of date or inapplicable and the ACISO must use substantial judgment in applying guidelines and determining relevance in most situations.

The ACISO adheres to various Federal mandates, such as the Federal Information Security Modernization Act of 2014 (FISMA), the Clinger-Cohen Act (CCA) of 1996, the Privacy Act of 1974, OMB Circular A-130, Appendix III, and Presidential Decision Directive 63 require high-level direction and coordination for information asset protection, Federal Information Technology Acquisition Reform Act (FITARA).

Factor 4 – Complexity

Level 4-6 (450 Points)

The ACISO manages and oversees the Bureau IT Security Program which involves establishing, implementing, and interpreting the requirements for Bureau compliance with Departmental policy directives and Executive Orders governing infrastructure protection of IT systems. The work is a critical component of the Department's mission and is comprised of multi-disciplinary and multi-functional activities. Assignments require that the incumbent have a thorough understanding of (1) Federal IT regulations, (2) a wide range of IT equipment, (3) varied information system types and respective hardware and software, and (4) security solutions required to support a variety of scientific, engineering, and administrative Bureau missions. The incumbent must identify current and potential security problems, develop new standards, methods, and techniques, and evaluate the impact of performance measure for gauging the effectiveness of the Bureau's Security Program.

Work is carried out with only very general review and consultation. The work requires a broad ability to analyze both policy and technical matters, to make decisions, to advise the ACIO and other executive level officials on major functional areas in the IT security modernization arena and to utilize representational skills. The incumbent must be able to represent the ACIO, and the Bureau, and speak with the authority to command the attention of people with varying agendas and interests. Representational skills are critical to spearhead the Federal Information Security Modernization Act (FISMA) of 2014.

The work involves participation as an expert authority for integrating IT security projects and efforts, and resolving problems and issues concerning all phases of IT security conception, planning, design, execution, and evaluation. Such work often involves overlapping and conflicting objectives and requirements that are difficult to resolve. Decisions and recommendations made require extensive consideration and analysis of very broadly defined or ill-defined issues and the establishment of new concepts and approaches will be required.

Alternatives and solutions may involve competing objectives. This work requires extensive coordination and support of other experts at the Department level and across the bureaus.

Another level of complexity is manifest in the requirement to incorporate Department multi-layered mission performance and organizational issues; operational compared with conceptual applications; quality and standardization concerns and approaches; numerous technical platforms to be considered; and the psychological and organizational roadblocks to technical transfer and change management. Recommendations regarding what is to be done involve largely undefined issues and elements, requiring extensive probing and analysis to determine the nature and scope of the problems. Then appropriate solutions must be planned and executed in an extremely dynamic environment due to the fact that computer and information security is a constantly evolving discipline, often requiring significant departures from previous approaches and extensions of traditional techniques, requiring development of new methodologies.

The ACISO manages and administers the Bureau IT Security Program; is responsible for developing policy, budgeting, and execution of such a program in compliance with mandates; develops directives required to implement legislation (e.g., Clinger-Cohen Act, Federal Information Security Modernization Act of 2014 (FISMA), etc.); represents the Bureau to the Department and other outside organizations (e.g., OIG, OMB, DHS, FBI, etc.); manages the IT security program review efforts including identifying systemic IT Security weaknesses and implementing internal controls. Computer and information security is a constantly evolving discipline, often requiring significant departures from previous approaches and extensions of traditional techniques, requiring development of new methodologies. The ACISO must use considerable judgement, forethought and tact to manage the Bureau IT security program in a way that meets requirements while not hampering mission activities.

Factor 5 - Scope and Effect

Level 5-5 (325 Points)

As the ACISO, the purpose of the work is to research, evaluate, plan, develop, and maintain the Bureau-wide IT Security Program. The work of this position has a major impact on Bureau IT resource decisions and actions nationwide. The effective accomplishment of the work drastically impacts essential business and mission-related processes within the Bureau, and has substantial impact on the Department, other Bureaus, stakeholders and private industry that deal with the Bureau.

The incumbent develops Bureau strategies, policies, procedures, and guidance via collaboration with other Bureau ACISOs, the Departmental CISO, other Government entities, oversight agencies, and Congress. In developing and implementing a Bureau IT Security Program, the ACISO must take into consideration the diverse business needs of Bureaus and offices while promoting a customer-centric approach to delivering services and support to both internal and

external customers and stakeholders while maintaining information integrity. The ACISO trains and monitors members of the IT Security community within Bureaus and offices and is the Bureau's primary agent for engaging the Department's business community in optimizing and transforming critical business processes to meet IT Security standards through structured process re-engineering efforts which provide seamless business and technological solutions to critical mission activities.

Factor 6 - Personal Contacts/Factor7- Purpose of Contacts Level 6-3 (d) (280 Points)

The ACISO has day-to-day personal contact with all levels of management in the Bureau and the Department, as well as in Bureau Headquarters and Regional Offices. Contacts also include information users, computer technicians, contract specialists, and Executive Leadership Team managers. There is contact with personnel from oversight agencies such as the Government Accountability Office, the General Services Administration, the Office of Management and Budget, the Office of Inspector General, contact and coordination with the Department of Homeland Security, the Federal Bureau of Investigation, recognized representatives at Federal, State, County and Municipal levels as well as congressional representatives.

Contacts are to propose solutions to significant problems and to recommend, justify and negotiate requirements, specification, resources, and needs in the management and security of information resources to obtain support, assistance, or coordination on IT security issues which have major organizational and/or resource implications. The ACISO: (1) briefs Bureau and Departmental officials, (2) establishes and maintains mutually beneficial consultative relationships with colleagues, (3) answers questions and concerns of oversight officials, (4) coordinates work efforts, (5) advises on IT Security Program plans, (6) coordinates with procurement, (7) establishes security safeguards, (8) obtains information for use in coordination of the Department's IT Security Program, (9) provides guidance on Federal IT security policies and regulations, and (10) obtains and disseminates information on Security Program technology. Many contacts involve sensitive or controversial issues on Bureau objectives, long-range planning, and major program decisions.

Factor 8 - Physical Demands

Level 8-1 (5 Points)

No unusual physical effort is required. The work is mainly sedentary, although some periods of frequent travel may be required.

Factor 9 - Work Environment

Level 9-1 (5 Points)

Work is performed primarily in an office setting.

Total Points: 4215

Points Range: 4055–up = GS-15

POSITION DESCRIPTION <i>(Please Read Instructions on the Back)</i>						1. Agency Position No. DOI1006	
2. Reason for Submission <input type="checkbox"/> Redescription <input checked="" type="checkbox"/> New <input type="checkbox"/> Reestablishment <input type="checkbox"/> Other		3. Service <input type="checkbox"/> Hdqtrs <input checked="" type="checkbox"/> Field		4. Employing Office Location		5. Duty Station	
Explanation <i>(Show any positions replaced)</i> Standard PD		7. Fair Labor Standards Act <input checked="" type="checkbox"/> Exempt <input type="checkbox"/> Nonexempt		8. Financial Statements Required <input type="checkbox"/> Executive Personnel Financial Disclosure <input type="checkbox"/> Employment and Financial Interest		9. Subject to IA Action <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
		10. Position Status <input checked="" type="checkbox"/> Competitive <input type="checkbox"/> Excepted <i>(Specify in Remarks)</i> <input type="checkbox"/> SES (Gen.) <input type="checkbox"/> SES (CR)		11. Position Is <input checked="" type="checkbox"/> Supervisory <input type="checkbox"/> Managerial <input type="checkbox"/> Neither		12. Sensitivity <input type="checkbox"/> 1--Non-Sensitive <input type="checkbox"/> 3--Critical <input type="checkbox"/> 2--Noncritical Sensitive <input checked="" type="checkbox"/> 4--Special Sensitive	
13. Competitive Level Code		14. Agency Use					
15. Classified/Graded by		Official Title of Position		Pay Plan		Occupational Code	
a. Office of Personnel Management							
b. Department, Agency or Establishment		Supervisory Information Technology Specialist (Security)		GS		2210	
c. Second Level Review							
d. First Level Review							
e. Recommended by Supervisor or Initiating Office							
16. Organizational Title of Position <i>(if different from official title)</i> Associate Chief Information Security Officer				17. Name of Employee <i>(if vacant, specify)</i>			
18. Department, Agency, or Establishment Department of the Interior				c. Third Subdivision			
a. First Subdivision Office of the Chief Information Officer				d. Fourth Subdivision			
b. Second Subdivision Bureau Associate Chief Information Officer				e. Fifth Subdivision			
19. Employee Review-This is an accurate description of the major duties and responsibilities of my position.				Signature of Employee <i>(optional)</i>			
20. Supervisory Certification. I certify that this is an accurate statement of the major duties and responsibilities of this position and its organizational relationships, and that the position is necessary to carry out Government functions for which I am responsible. This certification is made with the knowledge that				this information is to be used for statutory purposes relating to appointment and payment of public funds, and that false or misleading statements may constitute violations of such statutes or their implementing regulations.			
a. Typed Name and Title of Immediate Supervisor				b. Typed Name and Title of Higher-Level Supervisor or Manager <i>(optional)</i>			
Signature		Date		Signature		Date	
21. Classification/Job Grading Certification. I certify that this position has been classified/graded as required by Title 5, U.S. Code, in conformance with standards published by the U.S. Office of Personnel Management or, if no published standards apply directly, consistently with the most applicable published standards.				22. Position Classification Standards Used in Classifying/Grading Position			
Typed Name and Title of Official Taking Action Renae Lockwood, Sr. HR Specialist (Class/Comp)				OPM Job Family Standard for Administrative Work in the IT Group, 2200, September 2008, and May 2011; OPM GSSG, HRCD-5, dated June 1998 and April 1998.			
Signature RENAE LOCKWOOD		Digitally signed by RENAE LOCKWOOD Date: 2017.02.10 07:40:32 -05'00'		Date 02/10/2017		Information for Employees. The standards, and information on their application, are available in the personnel office. The classification of the position may be reviewed and corrected by the agency or the U.S. Office of Personnel Management. Information on classification/job grading appeals, and complaints on exemption from FLSA, is available from the personnel office or the U.S. Office of Personnel Management.	
23. Position Review		Initials Date		Initials Date		Initials Date	
a. Employee <i>(optional)</i>							
b. Supervisor							
c. Classifier							
24. Remarks							
25. Description of Major Duties and Responsibilities <i>(See Attached)</i>							

Instructions for Completing Optional Form 8

POSITION DESCRIPTION

In order to comply with the requirements of FPM Chapter 295, subchapter 3, and other provisions of the FPM, agencies must complete the items marked by an asterisk. Agencies may determine what other items are to be used.

- *1. Enter position number used by the agency for control purposes. See FPM Chapter 312, Subchapter 3.
- *2. Check one.
 - "Redescription" means the duties and/or responsibilities of an existing position are being changed.
 - "New" means the position has not previously existed.
 - "Reestablishment" means the position previously existed, but had been cancelled.
 - "Other" covers such things as change in title or occupational series without a change in duties or responsibilities.
 - The "Explanation" section should be used to show the reason if "Other" is checked, as well as any position(s) replaced by position number, title, pay plan, occupational code, and grade.
3. Check one.
- *4. Enter geographical location by city and State (or if position is in a foreign country, by city and country).
- *5. Enter geographical location if different from that of #4.
6. To be completed by OPM when certifying positions. (See Item 15 for date of OPM certification.) For SES and GS-16/18 positions and equivalent, show the position number used on OPM Form 1390 (e.g., DAES0012).
- *7. Check one to show whether the incumbent is exempt or nonexempt from the minimum wage and overtime provisions of the Fair Labor Standards Act. See FPM Chapter 551.
8. Check box if statement is required. See FPM Chapter 734 for the Executive Personnel Financial Disclosure Report, SF 278. See FPM Chapter 735, Subchapter 4, for the Employment and Financial Interests Statement.
9. Check one to show whether Identical Additional positions are permitted. See FPM Chapter 312, Subchapter 4. Agencies may show the number of such positions authorized and/or established after the "Yes" block.
10. Check one. See FPM Chapter 212 for information on the competitive service and FPM Chapter 213 for the excepted service. For a position in the excepted service, enter authority for the exception, e.g., "Schedule A-213.3102(d)" for Attorney positions excepted under Schedule A of the Civil Service Regulations. SES (Gen) stands for a General position in the Senior Executive Service, and SES (CR) stands for a Career Reserved position.
11. Check one.
 - A "Supervisory" position is one that meets the requirements for a supervisory title as set forth in current OPM classification and job-grading guidance. Agencies may designate first-level supervisory positions by placing "1" or "1st" after "Supervisory."
 - A "Managerial" position is one that meets the requirements for such a designation as set forth in current OPM classification guidance.
12. Check one to show whether the position is non-sensitive, noncritical sensitive, critical sensitive, or special sensitive for security purposes. If this is an ADP position, write the letter "C" beside the sensitivity.
13. Enter competitive level code for use in reduction-in-force actions. See FPM Chapter 351.
14. Agencies may use this block for any additional coding requirement.
- *15. Enter classification/job grading action.
 - For "Official Title of Position," see the applicable classification or job grading standard. For positions not covered by a published standard, see the General Introduction to "Position Classification Standards," Section III, for GS positions, or FPM Supplement 512-1, "Job Grading System for Trades and Labor Occupations," Part 1, Section III.
 - For "Pay Plan code, see FPM Supplement 292-1, "Personnel Data Standards," Book III.
 - For "Occupational Code," see the applicable standard; or, where no standard has been published, see the "Handbook of Occupational Groups and Series of Classes" for GS positions, or FPM Supplement 512-1, Part 3, for trades and labor positions. **For all positions in scientific and engineering occupations, enter the two-digit functional classification code in parentheses immediately following the occupational code, e.g., "GS-1310(14)."** The codes are listed and discussed in the General Introduction to "Position Classification Standards," Section VI.
16. Enter the organizational, functional, or working title if it differs from the official title.
17. Enter the name of the incumbent. If there is no incumbent, enter "vacancy."
- *18. Enter the organizational location of the position, starting with the name of the department or agency and working down from there.
19. If the position is occupied, have the incumbent read the attached description of duties and responsibilities. The employee's signature is optional.
- *20. This statement normally should be certified by the immediate supervisor of the position. At its option, an agency may also have a higher-level supervisor or manager certify the statement.
- *21. This statement should be certified by the agency official who makes the classification/job grading decision. Depending on agency regulations, this official may be a personnel office representative, or a manager or supervisor delegated classification/job grading authority.
22. Enter the position classification/job grading standard(s) used and the date of issuance, e.g., "Mail and File, GS-305, May 1977."
23. Agencies are encouraged to review periodically each established position to determine whether the position is still necessary and, if so, whether the position description is adequate and classification/job grading is proper. See FPM Letter 536-1 (to be incorporated into FPM Chapter 536). This section may be used as part of the review process. The employee's initials are optional. The initials by the supervisor and classifier represent recertifications of the statements in items #20 and #21 respectively.
24. This section may be used by the agency for additional coding requirements or for any appropriate remarks.
- *25. Type the description on plain bond paper and attach to the form. The agency position number should be shown on the attachment. See appropriate instructions for format of the description and for any requirements for evaluation documentation, e. g., "Instructions for the Factor Evaluation System," in the General Introduction to "Position Classification Standards," Section VII.

Department of the Interior
Supervisory Information Technology Specialist (Security)
Associate Chief Information Security Officer (ACISO)
GS-2210-15

I. Introduction

This is a standardized position description for the Department's Associate Chief Information Security Officers (ACISOs) located in the various Bureaus and Offices of the Department. The ACISO reports to the Bureau Associate Chief Information Officer (ACIO), and the Departmental Chief Information Security Officer (CISO) located in the Office of the Chief Information Officer (OCIO). The ACISO is accountable for collaboration on Departmental Information Technology (IT) Security policy and implementation of the Department's IT Security Program within their respective Bureau.

The ACISO serves as their assigned Bureau's senior subject matter expert and principal technical advisor and consultant to the ACIO, and is responsible for providing strategic leadership vision, direction, and coordination in support of Departmental IT Security Program activities across their assigned Bureau. This position is required for the protection of information and information systems and for providing a framework to manage and measure IT Security program performance, promote increased awareness throughout the Bureau, and to reduce potential breaches of sensitive Bureau information and the compromise of information systems.

II. Major Duties

Supervisory Duties 25%

The ACISO supervises a highly technical IT security team critical to the protection of Bureau and Departmental information assets. Supervision and oversight at this level requires exceptional coordination and integration of a number of segments or programs of technical work that could be politically sensitive and cause legal ramifications if not implemented properly. Supervision and management at this level involves major decisions and actions which have a direct and substantial effect on other organizations and programs in the Bureau and the Department. The supervision involves:

- Establishing IT Security projects, priorities, deadlines and goals.
- Planning and assigning work based on functions, priorities, complexity of assignment and capabilities and expertise of employees.

- Recommending promotion and/or reassignment of staff.
- Resolving informal complaints and group grievances.
- Reviewing and/or taking minor disciplinary action and makes recommendations to superiors on very serious or extensive actions.
- Developing performance standards and evaluating work performance of subordinates.
- Giving advice, counsel, or instruction to employees on both work and administrative matters.
- Interviewing and selecting candidates for highly technical positions.
- Identifying training and developmental needs of the staff.
- Approving leave and other common supervisory duties.

The ACISO is responsible for furthering the goals of equal employment opportunity (EEO) by taking positive steps to assure the accomplishment of affirmative action objectives and by adhering to nondiscriminatory employment practices in regard to race, color, religion, sex, national origin, age, or handicap. Specifically, ACISO initiates nondiscriminatory practices and affirmative action for the area under his/her supervision in the following: (1) merit promotion of employees and recruitment and hiring of applicants; (2) fair treatment of all employees; (3) encouragement and recognition of employee achievements; (4) career development of employees; and (5) full utilization of their skills.

IT Security Leadership: 25%

The ACISO serves as the senior subject matter expert, principal technical advisor, and consultant to the ACIO by providing strategic leadership vision, direction, and coordination in support of Departmental IT Security Program activities across the Bureau. The ACISO has primary responsibility on all matters pertaining to the security of information and information systems supporting Bureau assets including budget formulation and execution, security auditing, security awareness training, business security policy, and compliance reporting. The ACISO:

- Serves as principal Bureau liaison to the Department OCIO on all issues related to IT security.
- Manages an IT Security Office within the Bureau with the mission and resources necessary to ensure Departmental compliance with Section 3554 of FISMA.
- Provides expert guidance to senior agency officials concerning responsibilities under paragraph 3554 (a) (2) of FISMA.
- Serves as lead advisor in network and systems design to ensure implementation of appropriate systems security policies, advises on developing system security contingency plans and disaster recovery procedures.
- Provides expert technical, analytical, and managerial guidance for the planning, review, evaluation, implementation, coordination, and integration of IT Security requirements

within the Bureau's IT architecture.

- Promotes awareness of IT security issues among management and conducts security briefings and training to foster institutionalized awareness of the Bureau's Security Program and accepted security practices.
- Represents the Bureau on Federal government and industry committees, groups, and task forces concerned with security issues, policies, standards, guidance, and practices to address opportunities, challenges, or problems relating to IT and information management.
- Provides oversight to personnel with significant responsibilities for information security.

IT Security Policy Interpretation and Development: 25%

The ACISO has primary responsibility for the development of IT security policy within assigned Bureau that advances secure IT solutions and services residing on a reliable, secure, cost-efficient and effective supporting infrastructure. The ACISO exercises authority in the management, regulation, assessment, and reporting of Bureau IT security, and ongoing assessment for compliance with Department, Federal, and National Institute of Standards and Technology (NIST) policies, directives, guidelines, and best practices. The ACISO also has responsibility for reporting on the performance of the bureau-wide IT Security Program and the development of Bureau IT security policies and procedures. The ACISO:

- Directs development, develops, and maintains Bureau IT security policies, procedures, and guidance to ensure information systems confidentiality, integrity and availability, to prevent and defend against unauthorized access to systems, networks, and data systems, and to address all applicable requirements, including those issued under Section 3553 of FISMA, and Section 11331 of Title 40.
- Interprets Government-wide information security guidelines and establishes standards, policies, guidelines, and control techniques to ensure appropriate application, implementation, and compatibility of IT security on Bureau systems.
- Initiates, manages, coordinates, and assures maintenance of formal and informational documentation associated with the Bureau's IT Security Program.
- Establishes Bureau-wide IT Security education, awareness, and training for required employees and contractors.
- Collaborates with the Departmental CISO in development and/or revision of Department IT security policies and procedures.
- Ensures communication of and timely compliance with all Department IT security policies, procedures, and directions.
- Coordinates all Bureau activities in response to IT Security policies, procedures and directions including development and implementation of operational IT security activities, collection of information, and submission of reports.

- Participates on Government-wide advisory boards along with other cabinet level agencies to draft Governmental IT Security policy, and make Government-wide IT security recommendations.

IT Security Operations 25%

The ACISO has primary responsibility for ensuring Bureau information systems confidentiality, integrity and availability, and the prevention and defense against unauthorized access to systems, networks, and data. The ACISO oversees, manages, and provides coordination, technical guidance, and direction on all aspects of the IT security operations within the Bureau including:

- Coordinates implementation of the Departmental IT Risk Management Framework, Assessment and Authorization, and associated enterprise-wide continuous monitoring processes, procedures and programs to reduce the risk of vulnerabilities and weaknesses that could adversely impact the confidentiality, integrity or availability of sensitive agency information and information systems.
- Provides oversight in the monitoring of all Bureau systems development and operations for IT security compliance.
- Conducts risk and vulnerability assessments of planned and installed information systems to identify vulnerabilities, risks, and protection needs for the Bureau.
- Provides oversight to ensure Bureau IT components are assessed and authorized to fully meet Federal computer security requirements.
- Oversees systems security evaluations, audits, and reviews.
- Directs an IT security operations program by providing management and direction over contractor support tasks and work orders, identifying funding, manpower, and technical requirements and descriptions of the work to be accomplished; planning and establishing work schedules, deadlines, and standards for acceptable work; coordinating and integrating contractor work schedules and processes with the work of others; tracking progress and quality of performance; and deciding on the acceptability, rejection, or correction of work products or services, and similar matters which may affect payment to the contractor.
- Leads or oversees evaluations of IT security activities, provides briefings and recommendations to management on major IT security problems or issues discovered during evaluations, and develops comprehensive reports of findings and remediation actions.
- Maintains awareness of current developments in the area of IT security, information management and information technologies.
- Establishes and leads Computer Security Incident Response teams, and is the primary Bureau contact for all cybersecurity incidents.
- Maintains awareness of potential threats to the security and/or integrity of Bureau data;

stays abreast of threat activity to include computer viruses, patterns and methods of unauthorized intrusion in other government computer systems; communicates effectively and in a timely manner with all staff organizations regarding potential threats; conducts security briefings and other types of security training to foster an awareness of the IT Security Program throughout the Bureau.

- Oversees IT Security Audit and Risk Programs, conducting periodic evaluations and reviews to ensure the effective implementation of security safeguards and that the Security Program is in compliance with existing directives and appropriate to the risks and sensitivity of each computer application.
- Oversees a security monitoring program to ensure that security safeguards implemented within an information system are not circumvented.

Performs other related duties as assigned.

Condition of Employment

SPECIAL SENSITIVE (requiring Top Secret & SCI access) no waiver's allowed:

This position is designated as a SPECIAL SENSITIVE National Security position. Prior to appointment (Entrance on Duty), it requires a fully completed and favorably adjudicated National Security Background Investigation (SSBI or SSBI-PR) that is current (within the last 5 years). Once employed, further processing for special access approval (SCI) will also occur.

III. Supervisory Factors

Factor 1, Program Scope and Effect

Level 1-3, 550 Points

The coverage of the program is Bureau-wide and involves the management of a major aspect of a key agency technical program. The ACISO has primary responsibility for ensuring Bureau information systems confidentiality, integrity and availability, and the prevention and defense against unauthorized access to systems, networks, and data. The ACISO oversees, manages, and provides coordination, technical guidance, and direction on all aspects of the IT security operations within the Bureau. At this level, the information Security Program involves major decisions and actions which have a direct and substantial effect on other organizations and programs in the Bureau and the Department. Services provide direct and substantial services to the Bureau and indirectly to the Department. The IT security services provided are complex and require exceptional coordination and integration of a number of segments or programs of technical work that could be politically sensitive and cause legal ramifications if not implemented properly. Directs work which provides mission-supporting services that directly

impact a group of activities that include complex professional and administrative functions as well as complex, diverse technical functions.

Factor 2, Organizational Setting

Level 2-3, 350 Points

The ACISO performs his/her duties and responsibilities under the general administrative supervision of a Senior Executive (SES) or SES equivalent.

Factor 3, Supervisory and Managerial Authority Exercised

Level 3-3, 775 Points

In addition to making work assignments, tracking progress, and arbitrating disputes, the ACISO assists the CISO in the development and implementation of an agency-wide IT Security Program. The ACISO conducts the full range of supervisory duties including planning, prioritizing, and establishing deadlines for work; assigning and evaluating work; and seeking and implementing improved working conditions, methods of accomplishing work, and quality controls. Other human resources related responsibilities include preparing position descriptions; developing performance standards; recruiting, interviewing, and selecting staff; counseling staff; approving expenditures such as within-grade increases, overtime, and travel; and approving leave requests.

Factor 4, Personal Contacts

4A. Nature of Contacts, Level 4A-3, 75 Points

Contacts include executives and high level staffs throughout Bureau and Department, and other Federal agencies, and contractors. Contacts occur in a variety of settings such as meetings, conferences, and ad hoc events during which the ACISO serves as Bureau's point of contact and authority on IT Security Programs and issues.

4B. Purpose of Contacts, 4B-3, 100 Points

The purpose of contacts is to consult and negotiate with Bureau, and Department senior staff, provide advice and recommendations regarding project management and execution, present and defend significant or controversial findings and recommendations in regard to fundamental IT practices; in obtaining or committing resources, and in gaining/ensuring compliance with established policies, mandates, regulations, or contracts.

Factor 5, Difficulty of Typical Work Directed

Level 5-8, 1030 Points

The position supervises a staff of analysts performing technical IT security tasks. The highest grade that represents at least 25% of the workload directed is GS-13.

Factor 6, Other Conditions

Level 6-5b, 1225 Points

This position provides oversight that requires significant and extensive coordination and integration of a number of important IT Security projects. The position supervises highly technical work at the GS-13 level. Supervision and resource management involve major decisions and actions which have a direct and substantial effect on the Bureau and the programs managed.

Point Total: 4105

Point Range: 4055-up = GS-15