



United States Department of the Interior

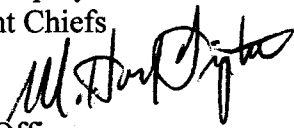
OFFICE OF THE SECRETARY
Washington, DC 20240




AUG 18 2004

Memorandum

To: Solicitor
Inspector General
Heads of Bureaus and Offices
Bureau and Office Chief Information Officers
Bureau and Office Deputy Chief Information Officers
Bureau Procurement Chiefs

From: W. Hord Tipton 
Chief Information Officer

Debra E. Sonderman, Director 
Office of Acquisition and Property Management

Subject: **Information Technology Security Requirements for Acquisition**

The Department of the Interior (DOI) relies heavily on information technology (IT) to accomplish its mission. Therefore, it is critical that our information be protected from uninvited disclosure or intentional corruption, and that our systems are secured against external attack to the maximum extent possible. This memorandum establishes guidance that will help assure that our contractors perform in a manner consistent with DOI's security needs and mandates.

IT security requirements must be incorporated into *all* phases of program planning and execution, from budgeting to close-out. The cognizant Program Manager or IT System Owner has primary responsibility to assure that contractors are aware of and comply with the DOI Security Program. However, support and cooperation from many disciplines, such as IT security, procurement, and legal, are required in order to apply and enforce security requirements effectively. Guidelines concerning performance of common tasks are enclosed. (Enclosure 1) These guidelines are intended to provide representative examples and stimulate thoughtful analysis, but are not comprehensive lists of every possible task that might arise.

Statements of Work (SOWs), or Performance Work Statements (PWSs), constitute the key element of a contract that communicates DOI's requirements or outcomes to the contractor. When a contractor is expected to design, develop, operate, use, or maintain a DOI IT system or access DOI information, we must take particular care to address IT security concerns in the solicitation and contract. We have developed a matrix to aid in this task. (Enclosure 2) As before, the matrix covers issues that often arise, but it may not be completely comprehensive. Program Managers and IT System Owners should use the matrix to develop SOWs and PWSs that are clear as to DOI's expectations and will result in an effective security program.

Effective immediately, all new IT and telecommunications related contracts must incorporate appropriate IT security requirements. Within six months, existing contracts must be reviewed for compliance with the DOI Security Program by the cognizant Program Manager or IT System Owner. Contracts that are found not to be in compliance must be modified as soon as possible, unless compliance is documented as being unreasonable or not cost effective when balanced against risk. Each bureau and office will report to the OCIO regarding the disposition of existing contracts no later than February 15, 2005.

Since each system will have a unique set of requirements or constraints, it is not possible to write standard language that applies to all contracts. However, as the Department gains more experience, we expect that some patterns of commonality will develop. In the future, we hope to be able to issue model language that will simplify the work of writing SOWs and PWSs.

Questions and suggestions related to this subject may be referred to Frank Menzer at (202) 208-5497 (IT issues) or Dee Emmerich at (202) 208 3348 (procurement issues).

Attachments

Guidelines to Program Manager or IT System Owner Tasks

- Identify IT security and privacy requirements during the requirements analysis phase based on a customized analysis of availability, integrity, and confidentiality; and the technical requirements of the contract.
- Use Federal Information Processing Standard 199 and the DOI Asset Valuation Guide to determine system sensitivity and criticality.
- Ensure that all hardware and software purchases conform to the current version of the DOI Technical Reference Model (see www.doi.gov/ocio/architecture).
- Ensure that all system development efforts comply with the best practices, technical standards, and product standards identified in the current version of the DOI Technical Reference Model (see www.doi.gov/ocio/architecture).
- Determine which IT security measures will be necessary to protect Sensitive but Unclassified (SBU) information by listing the potential threats and vulnerabilities, and then describing the measures needed to provide protection, including physical and environmental security safeguards.
- If information sharing is involved, resolve any conflicts among all affected information owners or custodians, and establish whatever MOUs or MOAs are necessary. In general, the information owner or custodian will establish the security level for their respective information.
- Develop specifications (either a Statement of Work or Performance Work Statement) that include appropriate IT security requirements and address appropriate technical, administrative, physical, and personnel security requirements.
- Develop evaluation criteria for use in the selection of the contractor.
- Participate in evaluation of the proposals received in response to the DOI procurement document to ensure that they address and meet the minimum IT security requirements and make a source selection recommendation.
- Undergo appropriate training to qualify as a Contracting Officer's Representative (COR), and serve as a COR as necessary.
- Prior to implementing any software configuration changes, obtain approval of the applicable Configuration/Change Control Board or Architectural Review Board. If no board exists, consult with the OCIO, Chief Technical Officer on the proper course of action.
- Prior to being moved into production, obtain approval of the applicable Technical Review

Board, Configuration/Change Control Board, Architectural Review Board for all software updates. Ensure the Independent Verification and Validation is performed. If no board exists, consult with the OCIO, Chief Technical Officer on the proper course of action.

- Ensure that periodic reviews of the project are conducted to ascertain whether IT security has been maintained at the appropriate level and compliance with the IT Security Program continued after award. All instances of noncompliance should be reported to the Contracting Officer, or designated representative, for necessary action.
- Conduct closeout activities, including return of all sensitive but unclassified information and IT resources provided during the life of this contract at the expiration or completion of this contract.

Guidelines to Contracting Officer Tasks

- Support the Program Manager or IT System Owner during the requirements analysis phase by conducting market research and providing procurement planning assistance as needed.
- Review incoming Statements of Work and Performance Work Statements for IT-related acquisitions to ensure that IT security has been addressed. If it has not, coordinate with the requisitioner to ensure compliance with the DOI IT Security Program.
- Include IT security as an evaluation factor in IT-related acquisitions, and ensure that IT security interests are represented during the evaluation period.
- Appoint Contracting Officer's Technical Representatives (COTRs) who are knowledgeable in IT security. If appropriate, appoint special COTRs with authority limited to IT security matters in addition to general COTRs.

Guidelines to IT Security Personnel Tasks

- Support the Program Manager or IT System Owner during the requirements analysis phase by evaluating requirements and providing advice on appropriate security measures.
- Review proposed Statements of Work and Performance Work Statements to ensure that the resulting contracts sufficiently define IT security responsibilities, provide a means to respond to IT security problems, and include a right to terminate the contract if it can be shown that the contractor does not abide by the IT security terms of the contract.
- Participate in evaluation of offers to ensure that IT security requirements are adequately addressed.
- Approve contractors' IT Certification and Accreditation documents in a timely manner.
- Undergo appropriate training to qualify as COTRs, and serve as COTRs as necessary.

If you are buying:				Put this requirement in the Statement of Work or constraint in the Performance Work Statement:
	COTS Hardware or Software	Development or Maintenance of Custom Applications	Outsourced IT Services or On-site Support	
1	N/A	✓	✓	<p>Background Investigation. Contractor employees who will have access to DOI information or will develop custom applications are subject to background investigations. The level/ complexity of background investigations must be the same as for a Federal employee holding a similar position; DM441, Chapter 3, provides guidance for the appropriate background investigations based on types of access. The solicitation and contract should state the levels required for applicable labor categories or positions.</p> <p>Ordinarily, the vendor should be responsible for paying the cost the background investigations. Existing clearances at the same or higher levels may be accepted. The request forms should be included in the solicitation if possible. Work cannot begin on the DOI system until the background investigation has at least been initiated.</p>
2	N/A	✓	✓	<p>Non-disclosure Agreement. Contractor employees who will have access to DOI information or will develop custom applications must sign a non-disclosure agreement prior to gaining access. Each agreement must be tailored to the contract, however, a sample agreement follows this matrix. A draft or sample agreement may be included in solicitations. After award, the COR will develop the final agreements, with the assistance of the Solicitor. Copies will be maintained in the contract file.</p>
3	N/A	✓	✓	<p>Training. Contractor employees must take DOI's end-user computer security awareness training prior to being granted access to DOI data or being issued a user account. Training must be renewed annually.</p>

4	N/A	N/A	✓	Personnel Changes. The contractor must notify the COR immediately when an employee working on a DOI system is reassigned or leaves the contractor's employ, and prior to an unfriendly termination.
5	N/A	✓	✓	Contractor Location. Custom software development and outsourced operations must be located in the United States to the maximum extent practical. If such services are proposed to be performed abroad, the contractor must provide an acceptable security plan specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the US may be an evaluation factor.
6	N/A	✓	N/A	Applicable Standards. Contractors must follow the DOI System Development Life Cycle (SDLC), NIST SP 800-64, and the DOI SDLC Security Integration Guide. Solicitations must include either the complete publications or a reference to public facilities, such as a website or office, where they may be accessed.
7	N/A	✓	✓	Asset Valuation. The Contractor must use the DOI Asset Valuation Guide for all systems to determine mission impact, data sensitivity, risk level, bureau/departmental/national criticality, and whether the system is a Major Application, Minor Application, or General Support System. Solicitations must include either the complete publication or a reference to public facilities, such as a website or office, where it may be accessed.
8	N/A	✓	✓	Property Rights. DOI will own the intellectual property rights to any software developed on its behalf to the maximum extent practical. Generally, FAR 52.227-14, Rights in Data-General, and its alternates will be used in the contract. However, deviation from this policy may be necessary as circumstances warrant.
9	N/A	✓	✓	IV&V. Software updates must be independently verified and validated prior to being moved into production. The solicitation and contract should be clear as to which party performs this function and is responsible for associated costs.

10	N/A	✓	✓	<p>Certification and Accreditation. Major Applications and General Support Systems must be certified and accredited (C&A) prior to going into production and re-accredited every three years or whenever there is a major change that affects security. C&A documents will be provided to the COR in both hard copy and electronic (specify) forms. The contractor must follow NIST SP 800-37, 800-18, 800-30, 800-60, 800-53, 800-53A, Federal Information Processing Standard (FIPS) 199 and 200, the associated DOI guides/templates, the DOI Security Test & Evaluation (ST&E) Guide, and the DOI Privacy Impact Assessment. Solicitations must include either the complete publications or a reference to public facilities, such as a website or office, where they may be accessed.</p> <p>The government will reserve the right to conduct the ST&E, using either Government personnel or an independent contractor.</p> <p>The contractor will take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.</p> <p>The Designated Approving Authority for the system will be the official identified in DOI Secretarial Order No. 3255.</p>
11	N/A	N/A	✓	<p>Internet Logon Banner. A Government-approved logon banner must be displayed on the first page of any public access web pages.</p>
12	N/A	✓	✓	<p>Incident Reporting. The contractor must report computer security incidents affecting DOI data or systems in accordance with the DOI Computer Incident Response ___ Guide. Solicitations must include either the complete publication or a reference to public facilities, such as a website or office, where it may be accessed.</p>
13	✓	✓	✓	<p>Quality Control. All software and hardware must be free of malicious code.</p>

14	N/A	N/A	✓	<p>Self Assessment. The contractor must conduct an annual self assessment in accordance with NIST SP 800-26 on all MAs, GSSs, and outsourced applications in production. Solicitations must include either the complete publication or a reference to public facilities, such as a website or office, where it may be accessed. Both hard copy and electronic copies of the assessment will be provided to the COR.</p> <p>The government will reserve the right to conduct such an assessment using Government personnel or another contractor.</p> <p>The contractor will take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.</p>
15	N/A	✓	✓	<p>Vulnerability Analysis. All systems must be scanned monthly with a vulnerability analysis tool that is compatible with the software in use by the OCIO at the time (specify this in the solicitation). All “safe” or “non-destructive” checks must be turned on. All electronic copy of each report and session data will be provided to the COR.</p> <p>At least annually, all high risk systems and systems accessible from the Internet must be independently penetration tested. Electronic and hard copy reports of penetration test results will be provided to the COR.</p> <p>The government will reserve the right to conduct un-announced and prearranged independent vulnerability scans using Government personnel or another contractor.</p> <p>The contractor will take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.</p>
16	N/A	✓	✓	<p>Logon Banner. Contractor employees who will access DOI data must acknowledge a Government-approved logon warning prior to each logon to the system.</p>

17	N/A	✓	✓	<p>Security Controls. Contractors will be required to ensure compliance with the security control requirements of the current version of NIST SP 800-53 (even if it is in draft) or Federal Information Processing Standard (FIPS) 200 that are appropriate to the sensitivity and criticality of the data or system. FIPS199 and the DOI Asset Valuation Guide will be used to determine sensitivity and criticality. Solicitations must include either the complete publications or a reference to public facilities, such as a website or office, where they may be accessed.</p>
18	N/A	N/A	✓	<p>Contingency Plan. The contractor will submit a contingency plan in accordance with NIST SP 800-34 and the DOI Contingency Plan Guide. Solicitations must include either the complete publications or a reference to public facilities, such as a website or office, where they may be accessed. The plan must be approved by the COR. A copy of the annual test results will be provided to the COR.</p>