Department of Transportation
Office of the Senior Procurement Executive

No. APL- 2012-03
Date 05/21/2012

DOT ACQUISITION POLICY LETTER

This Acquisition Policy Letter issued under the authority of the Senior Procurement Executive of the Department of Transportation

Subject: **Interim Contract Clause 1252-239-70 - Cybersecurity Requirements for Unclassified and Sensitive Information (June 2012)**

References:

- Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C § 3541 et seq.
- Clinger-Cohen Act of 1996 (also known as the "Information Technology Management Reform Act of 1996)," 40 U.S.C § 1401 et seq.
- Privacy Act of 1974, 5 U.S.C. § 552a, as amended.
- Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," and Appendix III, "Security of Federal Automated Information Systems," as amended.
- OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies."
- Homeland Security Presidential Directive (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004.
- DOT Order 1351.37, "Departmental Cybersecurity Policy."

When is this Acquisition Policy Letter (APL) Effective?

This APL is effective June 1, 2012.

When Does This APL Expire?

This APL remains in effect until the resulting policy is incorporated into the Transportation Acquisition Regulation (TAR) or otherwise cancelled.

Who is the Point of Contact?

Contact Jeffrey Thomas of the Office of the Senior Procurement Executive, (202) 366-4226 or by email at Jeff.Thomas@dot.gov. For technical questions regarding the implementation of the clause requirements, contact Arvid Knutsen of the Office of Cybersecurity and Information Assurance, at (202) 366-6115 or by email at arivd.knutsen@dot.gov.

Visit our website at http://www.dot.gov/ost/m60/ for additional information on DOT Acquisition Policy Letters and other policy issues.

What is the Purpose of this APL?

The purpose of the APL is to replace TAR Clause 1252.239-70 – Security Requirements for Unclassified Information Technology Resources (2005), with the updated interim TAR clause 1252.239-70 (June 2012) – Cybersecurity Requirements for Unclassified and Sensitive Information Technology (IT) Resources (2011).

The updated clause supports implementation of a number of Government and Department-wide policies related to cybersecurity for unclassified and sensitive IT resources.

This APL applies to all Department of Transportation (DOT) operating administrations except the Federal Aviation Administration (FAA). The FAA is responsible for implementation of required IT security requirements through the FAA Acquisition Management System, or other Agency implementation policies and directives.

What is the Background?

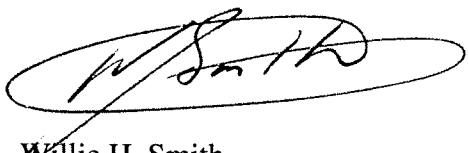
The Federal Information Security Management Act (FISMA) of 2002 requires federal agencies to identify and provide security protection commensurate with the risk and magnitude of potential harm resulting from the loss, misuse of, unauthorized access to, disclosure of, disruption to, or modification of information collected by or maintained on behalf of the agency. This protection is required for the information and information systems that support DOT's mission, operations and assets, including those provided or managed by another Federal agency, contractor, grantee, or other source. Consistent with the Departmental Cybersecurity Strategic Plan, and the Departmental Cybersecurity Policy (DOT Order 1351.37), cybersecurity policy is reviewed at least annually to ensure continued alignment with strategic and tactical objectives, responsiveness to evolving threats, incorporation of new cybersecurity requirements, and to address audit findings and recommendations. In response to these drivers, the Office of the Senior Procurement Executive (M-60), in cooperation with the DOT Chief Information Officer, updated TAR clause 1252.239-70 "Security Requirements for Unclassified Information Technology Resources (June 2012)" to reflect contemporary cybersecurity policy and practices, and agency-specific guidance. This revised interim TAR clause describes current requirements for ensuring security protections of information and information systems, new procedures, and provides clarification of the contractor's role and responsibilities in ensuring the security of information technology products and services provided to the government.

What is the Guidance?

1. Effective immediately, contracting officers shall insert the interim TAR clause 1252.239-70 "Cybersecurity Requirements for Unclassified and Sensitive Information Technology Resources (June 2012)" into all new solicitations and any resulting contracts (including Task Orders, if appropriate), exceeding the

micro-purchase threshold, where the contractor will develop, manage or operate IT systems connected to a DOT Network or for any contracted system that contains DOT information, regardless of location.

2. The contracting officer, in cooperation with the COTR and the Operating Administration (OA) chief information officer, shall review existing contracts exceeding the micro-purchase threshold (including Task Orders, if appropriate) where the contractor develops, manages or operates IT systems connected to a DOT Network or for any contract system that contains DOT information, regardless of location, to determine if the contract should be modified to add the updated clause. The determination to update the clause should be made as soon as practicable. As a minimum, this determination should be made prior to the exercise of any option periods of covered contracts. Where the contracting officer, in cooperation with the COR and the Operating Administration chief information officers, determine that the contract will not be modified to include the updated clause, a memorandum shall be placed in the contract file documenting the basis for the decision.



Willie H. Smith,
Senior Procurement Executive

Attachment

12-52239-70 CYBERSECURITY REQUIREMENTS FOR UNCLASSIFIED AND SENSITIVE INFORMATION TECHNOLOGY (IT) RESOURCES
(June 2012)

(a) Required Policies and Regulations - Compliance with applicable Federal statutes, policies, standards, and guidelines is the responsibility of the Federal government and may not be abdicated to the Contractor. To achieve such compliance, the government requires the Contractor to conform to all U. S. Department of Transportation (DOT) and applicable Federal IT Security statutes, policies, standards, and reporting requirements, including, but not limited to:

(1) Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C § 3541 et seq.

(2) Clinger-Cohen Act of 1996 also known as the "Information Technology Management Reform Act of 1996," 40 U.S.C § 1401 et seq.

(3) Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

(4) Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," and Appendix III, "Security of Federal Automated Information Systems," as amended.

(5) OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies."

(6) Homeland Security Presidential Directive (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004.

(7) DOT Order 1351.37, "Departmental Cybersecurity Policy."

(8) DOT Departmental Cybersecurity Compendium "Supplement to DOT Order 1351.37: Departmental Cybersecurity Policy."

(9) DOT Order 1681.1, "Department of Transportation (DOT) Implementation Policy for Identity, Credential, and Access Management (ICAM) and Homeland Security Presidential Directive - 12 (HSPD-12)."

(10) National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication (PUB) 140, "Security Requirements for Cryptographic Modules."

(11) NIST FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems."

(12) NIST FIPS PUB 200, "Minimum Security Requirements for Federal Information and Information Systems."

(13) NIST FIPS PUB 201, "Personal Identity Verification (PIV) of Federal Employees and Contractors" and all related NIST Special Publications.

(14) NIST Special Publication 800-18, "Guide for Developing Security Plans for Federal Information Systems."

(15) NIST Special Publication 800-30, "Risk Management Guide for Information Technology Security Risk Assessment Procedures for Information Technology Systems."

(16) NIST Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems."

(17) NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems."

(18) NIST Special Publication 800-47, "Security Guide for Interconnecting Information Technology Systems."

(19) NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems."

(20) NIST Special Publication 800-53A, "Guide for Assessing the Security Controls in Federal Information Systems."

(21) NIST Special Publication 800-63, "Electronic Authentication Guidance."

(b) Applicability - The Contractor shall be responsible for Information Technology security for all systems connected to a DOT network operated by the Contractor for DOT, or for Contractor Systems that contains DOT information regardless of location. The term Information Technology, as used in this clause, means any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For purposes of this definition, equipment is used by DOT whether DOT uses the equipment directly or it is used by a contractor under a contract with the agency which (1) requires the use of such equipment or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. Information Technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. It does not include any equipment acquired by a Federal contractor incidental to a Federal contract.

(c) Security Categorization - In accordance with FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems," DOT has determined that the security category of the information or information system under this contract is Confidentiality [Indicate LOW, MODERATE, or HIGH)], Integrity [Indicate LOW, MODERATE, or HIGH)], Availability [Indicate LOW, MODERATE, or HIGH)] with an overall security impact level of [Indicate LOW, MODERATE, or HIGH)].

(d) Baseline Security Controls and System Security Plan – The Contractor shall develop and maintain the System Security Plan and associated Baseline Security Controls for the system as defined in the DOT Departmental Cybersecurity Compendium. To aid DOT senior officials and Contractors in determining applicable security controls, the Departmental Cybersecurity Compendium assigns security requirements (also referred to as controls and policy) to the DOT Component and Information System levels. The Contractor is responsible for all "System-level" security requirements in accordance with the FIPS PUB 199 Categorization approved for the system unless otherwise indicated in the Statement of Work or Performance Work Statement. The Contractor shall follow DOT policy and guidance specified in DOT Order 1357.31 and the Departmental Cybersecurity Compendium to appropriately tailor the set of baseline security controls and define the implementation owner of each control. The Contractor shall obtain the written approval of the System Security Plan and corresponding Baseline Security Controls from the DOT Authorizing Official or his/her designee.

(e) Information System Contingency Plan (ISCP) and Testing -- The Contractor shall develop and maintain the ISCP for the system as defined in the DOT Departmental Cybersecurity Compendium. The Contractor shall regularly test the ISCP and document test results in accordance with the DOT Departmental Cybersecurity Compendium.

(f) Security Assessment and Authorization – All applicable Contractor systems/applications must support risk management processes, and produce and maintain the documents and artifacts as specified in the DOT Departmental Cybersecurity Policy and the DOT Departmental Cybersecurity Compendium. The Contractor shall prepare and submit the required documents as specified in the Deliverables section of the contract. For systems categorized as High or Moderate security impact per FIPS PUB 199, the Contractor must obtain a qualified independent Security Control Assessor and obtain the approval of this assessor from the DOT Authorizing Official. The Contractor may not begin the processing of DOT information, interconnecting with DOT networks or systems, or any other production operation of the system until the DOT Authorizing Official grants security authorization in accordance with DOT policy and procedures specified in the Departmental Cybersecurity Policy and Compendium.

(g) Continuous Monitoring - Upon attainment of security authorization from the DOT Authorizing Official, the Contractor must implement and perform continuous monitoring of the security state and controls of the information system as specified in the Departmental Cybersecurity Policy and Compendium producing the specified reports and other artifacts to demonstrate ongoing risk management.

(h) Contract Compliance - Upon approval by DOT, the Systems Security Plan, FIPS 199 Categorization, Contingency Plan, Security Assessment Report, Security Authorization, Plan of Action and Milestones (including any required updates), and other documents that are required based on the type of information system in accordance with the Departmental Cybersecurity Policy and Compendium, shall be incorporated into the contract file as compliance documents.

(i) Availability of Data, Documents and Access –

(1) The Contractor shall ensure that all DOT data remains within the United States except as approved in writing by the DOT Authorizing Official or his/her designee.

(2) The Contractor shall provide DOT (or DOT- designated third party contractors) access to the Contractor's and subcontractors' facilities, installations, operations, documents, records, databases, and personnel used in performance of the contract. The Contractor shall have the means to support DOT's request for access 24 hours per day, 7 days per week which may be necessitated due to a security incident, breach or other security matter.

(3) The Contractor shall provide access to the extent required to carry out IT security inspections, investigations, and/or audits to safeguard against threats and hazards to the integrity, availability, and confidentiality of DOT information or to the functions of information technology operated on behalf of DOT, and to preserve evidence of criminal activity.

(4) Upon termination of the contract or earlier, upon request, the Contactor shall provide to the DOT Authorizing Official or his/her designee all DOT data, source code, or database files, in a format specified by the DOT Authorizing Official or his/her designee.

(j) Monthly Deliverables: The Contractor shall provide, on a monthly basis, the following information in NIST Security Content Automation Protocols (SCAP) XML data formats:

(1) Device inventory (type of device and software);

(2) Medium and High Vulnerabilities for each device;

(3) Deviations from approved Configuration Baselines for each device; and

(4) Additional information as required by OMB or the Department of Homeland Security (DHS) as indicated in the Departmental Cybersecurity Compendium.

(k) Quarterly Deliverables: The Contractor shall provide, on a quarterly basis, the following information in a format specified by the COTR:

(1) Plan of Action and Milestones (POA&M) – The Contractor shall prepare a draft of the POA&M associated with known weaknesses at the completion of the initial security assessment. The Contractor shall collaborate with the DOT System Owner, Information System Security Officer/Manager (ISSO/ISSM) and DOT Authorizing Official to obtain necessary information to complete the POA&M to meet DOT guidelines specified in the DOT Departmental Compendium. The POA&M approved by the DOT Authorizing Official shall be included in the initial authorization package. Upon entering Continuous Monitoring phase, the Contractor shall update the POA&M at least quarterly to ensure it contains all known system security weaknesses discovered through security assessment, continuous monitoring, internal and external audits, and related activities that examine security and IT

controls of the contractor information system. The POA&M update shall also include progress on corrective actions for weaknesses previously identified.

(l) Annual Deliverables: The Contractor shall provide, on an annual basis, the following documents to the contracting officer and COTR:

1. Updated security risk management documentation:

   a. System Security Plan - The Contractor shall review and update the System Security Plan at least annually to ensure the plan is current, accurately describes implemented system controls and reflects changes to the Contractor system and its environment of operation.

   b. Security Assessment Report - The Contractor shall provide an update to the Security Assessment Report, based on the results of continuous monitoring performed. For systems categorized as High and Moderate security impact level, the independent Security Control Assessor must issue this report.

   c. Information System Contingency Plan (ISCP) - The Contractor shall provide an annual update to the ISCP completed in accordance the Departmental Cybersecurity Compendium.

   d. FIPS PUB 199 Categorization – The Contractor shall provide an update to the FIPS PUB 199 Categorization which shall identify any and all information type changes and resulting security impact levels for Confidentiality, Integrity and Availability in accordance with the DOT Departmental Cybersecurity Compendium. The DOT Authorizing Official must approve all changes in FIPS PUB categorization.

(2) Information Security Awareness and Training Records – The Contractor shall ensure its personnel complete both general awareness training and role-based training for personnel that perform roles deemed by DOT to require annual specialized security training (refer to Compendium Appendix D). The Contractor shall comply with awareness and training policy specified in the DOT Departmental Cybersecurity Compendium and evidence of completion of training shall be provided to the COTR upon request by the Government.

(3) Information System Interconnection Agreements – The Contractor shall identify all interconnections between its system and other parties. (Refer to the DOT Departmental Cybersecurity Compendium for definitions and requirements for documentation, security controls and authorization of interconnections).

(4) All Other Applicable Documents as Specified in the Departmental Cybersecurity Compendium.

(m) HSPD-12 / Identity, Credential and Access Management Requirements – The Contractor shall ensure, at a minimum, that all systems that it develops for or operates on behalf of the Government support the use of Personal Identity Verification (PIV) smart cards, and PIV interoperable (PIV-I) smart cards as appropriate, for authentication and access to those systems, for the digital signature of documents and workflows, and for the encryption of documents and information, in accordance with NIST PUB 201 and related special publications. When explicitly required, or by September 30, 2012, whichever occurs earlier, the Contractor shall ensure that all systems it develops for or operates on behalf of the Government meet applicable DOT policy requirements for identity, credential, and access management (ICAM) and require the use of a PIV card or PIV-I for authentication, access, digital signature, and encryption. The Contractor shall ensure that services and products it purchases involving facility or system access control are on the current FIPS 201 Approved Products List, found at http://www.idmanagement.gov/.

(n) US Government Configuration Baseline - The Contractor shall certify applications are fully functional and operate correctly as intended on systems using the US Government Configuration Baseline (USGCB). This includes Internet Explorer configured to operate in Windows. The standard installation, operation, maintenance, updates, and/or patching of software shall not alter the configuration settings from the approved USGCB configuration. The information technology should also use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges. The Contractor shall use Security Content Automation Protocol (SCAP) validated tools with USGCB Scanner capability to certify their products operate correctly with USGCB configurations and do not alter USGCB settings, and shall provide documentation of such validation to the Government as a prerequisite for Government acceptance of the Contractor's products. The Contractor shall follow guidance in the DOT Departmental Cybersecurity Compendium for tracking and reporting deviations from these baselines.

(o) System Access Notice - The Contractor shall implement DOT- approved warning banners on all DOT systems (both public and private) operated by the Contractor prior to allowing authenticated access to the system(s). The DOT Departmental Cybersecurity Compendium specifies requirements for this warning banner and permitted deviations depending on the end user device.

(p) Privacy Act Notifications - As prescribed in the Federal Acquisition Regulation (FAR) clause 24.104, if the system involves the design, development, or operation of a system of records on individuals, the Contractor shall implement requirements in FAR clause 52.224-1, "Privacy Act Notification" and FAR clause 52.224-2, "Privacy Act." The Contractor shall ensure that the following banner is displayed on all DOT systems that contain Privacy Act information operated by the Contractor prior to allowing anyone access to the system:

"This system contains information protected under the provisions of the Privacy Act of 1974 (Public Law 93-579). Any privacy information displayed on the screen or printed shall be protected from unauthorized disclosure. Individuals who violate privacy safeguards may be subject to disciplinary actions, a fine of up to $5,000, or both."

(q) Non-Disclosure Agreements - The Contractor shall cooperate in good faith in defining non-disclosure agreements that other third parties must sign when acting as the Federal government's agent.

(r) Nondisclosure of Security Safeguards - In accordance with the Federal Acquisitions Regulations (FAR) clause 52.239-1, the Contractor shall be responsible for the following privacy and security safeguards: the Contractor shall not publish or disclose in any manner, without the contracting officer's written consent, the details of any safeguards either designed or developed by the Contractor under the contract. If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

(s) Subcontracts - The Contractor shall incorporate the substance of this clause in all subcontracts that meet the conditions described in paragraph (b).

INTEROFFICE MEMORANDUM

TO: WILLIE SMITH

FROM: JEFFREY THOMAS

SUBJECT: ACQUISITION POLICY LETTER – INTERIM CONTRACT CLAUSE 1252-239-70 – CYBERSECURITY REQUIREMENTS FOR UNCLASSIFIED AND SENSITIVE INFORMATION (JUNE 2012)

DATE: 5/15/2012

CC:

Enclosed for your signature is APL - 2012-03 – Interim Contract Clause 1252-239-70 – Cybersecurity Requirements for Unclassified and Sensitive Information (June 2012). This APL supports implementation of a number of Government-Wide and Departmental policy updates related to cybersecurity for unclassified and sensitive IT resources.

The purpose of this APL is to provide an updated contract clause for use in all new solicitations and resulting contracts, exceeding the micro-purchase threshold, where the contractor will develop, manage, or operate IT systems connected to a DOT network or for any contracted system that contains DOT information, regardless of location. The APL is applicable to all operating administrations, except the FAA which is responsible for implementation of the required IT security requirements through FAA Acquisition Management System, or other implementation policies and directives.

The implementation of the policy and clause language was developed through an ad hoc working group with primary representation from the Office of the Senior Procurement Executive, Office of the Chief Information Officer, and the Office of Chief Counsel.

The final package has been reviewed and concurred by Office of the Chief Information Officer, and the Office of Chief Counsel.

5/18/12 - see e-mail for response to questions

Department of Transportation
Office of the Senior Procurement Executive

No. APL- 2012-03
Date 05/17/2012

DOT ACQUISITION POLICY LETTER

This Acquisition Policy Letter issued under the authority of the Senior Procurement Executive of the Department of Transportation

Subject: **Interim Contract Clause 1252-239-70 - Cybersecurity Requirements for Unclassified and Sensitive Information (June 2012)**

References:

- Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C § 3541 et
- Clinger-Cohen Act of 1996 (also known as the "Information Technology Management Reform Act of 1996)," 40 U.S.C § 1401 et seq.
- Privacy Act of 1974, 5 U.S.C. § 552a, as amended.
- Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," and Appendix III, "Security of Federal Automated Information Systems," as amended.
- OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies."
- Homeland Security Presidential Directive (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004.
- DOT Order 1351.37, "Departmental Cybersecurity Policy."

When is this Acquisition Policy Letter (APL) Effective?

This APL is effective June 1, 2012.

When Does This APL Expire?

This APL remains in effect until the resulting policy is incorporated into the Transportation Acquisition Regulation (TAR) or otherwise cancelled.

Who is the Point of Contact?

Contact Jeffrey Thomas of the Office of the Senior Procurement Executive, (202) 366-4226 or by email at Jeff.Thomas@dot.gov. For technical questions regarding the implementation of the clause requirements, contact Arvid Knutsen of the Office of Cybersecurity and Information Assurance, at (202) 366-6115 or by email at arivd.knutsen@dot.gov.

Visit our website at http://www.dot.gov/ost/m60/ for additional information on DOT Acquisition Policy Letters and other policy issues.

CONCURRENCES

RTG SYMBOL	S-83
INITIALS/SIG	[illegible]
DATE	5/7/2012
RTG SYMBOL	C-10
INITIALS/SIG	[illegible]
DATE	5/14/12
RTG SYMBOL	M-61
INITIALS/SIG	[illegible]
DATE	5/15/12
RTG SYMBOL	
INITIALS/SIG	
DATE	
RTG SYMBOL	
INITIALS/SIG	
DATE	
RTG SYMBOL	
INITIALS/SIG	
DATE	
RTG SYMBOL	
INITIALS/SIG	
DATE	
RTG SYMBOL	
INITIALS/SIG	
DATE	

GRID