CIOP CHAPTER 37

Departmental Cybersecurity Policy

TABLE OF CONTENTS

Section 37.1 Purpose

The Departmental Cybersecurity Policy establishes the policies, processes, procedures and standards of the Department of Transportation (DOT) Information Systems Security Program, hereafter referred to as the Departmental Cybersecurity Program. The Departmental Cybersecurity Policy implements the requirements specified for all Federal agencies in the Federal Information Security Management Act (FISMA) of 2002 and related laws, regulations, and other mandatory guidance and standards related to information security, information assurance, and network security.

The DOT Office of the Chief Information Officer (OCIO), under the responsibility and authority granted by the Secretary of Transportation under Public Law 104-106, *Clinger-Cohen Act of 1996*, the Federal Information Security Management Act (FISMA) of 2002 and the Office of Management and Budget (OMB) Memo M-09-02, *Information Technology Management Structure and Governance Framework*, issues this policy to ensure that the Departmental Cybersecurity Program is developed, documented, and implemented to provide security for all DOT information systems, information technology, networks, and data that support DOT operations.

All DOT Operating Administrations (OA) and the Office of the Inspector General (OIG), hereafter referred to as DOT Components, must implement and comply with the policies specified herein to ensure:

i) the protection of DOT information systems and the sensitive data they contain from unauthorized access, use, disclosure, disruption, modification, or destruction from threats that can impact confidentiality, integrity and availability of the information, information technology services, and communications; and

ii) compliance with mandatory security-related laws, regulations and guidance.

The Departmental Cybersecurity Policy serves as the overarching, foundational directive for cybersecurity for DOT and authorizes the DOT Chief Information Officer (CIO) to develop and disseminate supplemental policies, guidance, procedures, standards and processes that implement mandatory cybersecurity requirements required of DOT by other entities. These entities include, but are not limited to, Congress, OMB, the National Institute of Standards and Technology (NIST), and the Department of Homeland Security (DHS). This collection of supplemental policies and guidance is collectively referred to as the Departmental Cybersecurity Compendium. The Departmental Cybersecurity Compendium:

- Incorporates and cross-references cybersecurity requirements and national standards, such as NIST Special Publication (SP) 800-53, according to information assurance control families in a manner that clearly presents scope and applicability.
- Presents all DOT cybersecurity directives in a manner that enables DOT stakeholders to scale and supplement baseline Departmental directives to meet unique requirements, if necessary.
- Exists as a living document, subject to additions, deletions, and/or content modifications based on changing requirements, technology, and threats, as deemed necessary by the DOT CIO.

If no DOT specific guidance exists on a specific cybersecurity area, the relevant Government-wide policy, guidance or standard is DOT policy unless otherwise specified by the DOT OCIO.

Increasing cybersecurity threats require DOT to frequently update its methodology for monitoring networks, detecting potential risks, identifying malicious activity, and mitigating threats to protect sensitive information and information systems. The implementation of the Departmental Cybersecurity Policy, coupled with the Departmental Cybersecurity Compendium, will facilitate DOT's ability to expedite the dissemination and implementation of DOT security measures to maintain currency, applicability, and effectiveness as requirements, environments, and threats change.

This document does not supersede any other applicable law such as FISMA or higher level Government-wide directive, policy, or guidance such as OMB circulars and memoranda. This document and the companion Departmental Cybersecurity Compendium are subject to periodic revision, update, and reissuance.

(Table of Contents)

Section 37.2 Background

The increasing threat of sophisticated cyber attacks requires a substantial enhancement of the security of DOT's digital infrastructure. Cyber threats originate in unfriendly nation-states, international criminal syndicates, and even within the United States (U.S.). As a result, DOT must be prepared at all times to manage these threats in a manner that minimizes their negative impact.

The organizations within the Federal Government charged with establishing information security policy, guidance, and standards, such as OMB, NIST and DHS, provide direction to Federal government agency officials through a number of means. Recent guidance from OMB and NIST dramatically changes the manner in which executive agencies must identify and manage risk associated with information systems. This DOT Order implements the responsibilities and methods described as the NIST Risk Management Framework (RMF) which specifies that:

- DOT senior leaders/executives must be committed to making risk management a fundamental mission/business requirement. This top-level, executive commitment ensures sufficient resources are available to develop and implement effective, organization-wide risk management programs.
- Understanding and addressing risk is a strategic capability and an enabler of missions and business functions across DOT.
- Effectively managing information security risk DOT-wide requires assignment of risk management responsibilities to senior leaders/executives.
- There must be ongoing recognition and understanding by senior leaders/executives of the information security risks to DOT operations and assets, individuals, other organizations, and the Nation arising from the operation and use of information systems.

- DOT must establish its tolerance for risk and communicate the risk tolerance throughout the organization including guidance on how risk tolerance impacts ongoing decision-making activities.
- DOT senior leaders/executives must be provided clear and concise information to enable them to effectively carry out their risk management responsibilities to be accountable for risk management decisions and for the implementation of effective, risk management programs within their organizations.

DOT's Cybersecurity Strategic Plan addresses cybersecurity through the Departmental Cybersecurity Program that targets ways to maintain and improve the robustness, resiliency, safety, and efficiency of the DOT digital infrastructure to protect departmental information system assets. Implementing and tracking the progress of the DOT Cybersecurity Strategic Plan through the DOT Cybersecurity Program and supporting the Departmental Cybersecurity Compendium will enhance the organizational excellence of DOT and the effectiveness of DOT Components. DOT's Departmental Cybersecurity Program must continually evolve and mature to:

- Address new and changing Federal regulations and requirements,
- Support advances in technology and information technology service delivery, and
- Detect and combat new threats to the Department's information systems and supporting infrastructure.

Evolution of the Departmental Cybersecurity Policy and its companion Departmental Cybersecurity Compendium must be executed in a manner that:

- Responds to mandatory national cybersecurity policies and standards, technological advances, and emerging threats and
- Streamlines additions to, and modifications of, new and changing cybersecurity requirements and mitigation strategies.

(Table of Contents)

Section 37.3 Scope and Applicability

37.3.1 Title III of the E-Government Act, known as FISMA, requires each Federal department and agency to develop, document, and implement an agency-wide information cybersecurity program to provide information security for the information and information systems that support the operations and assets of the agency.

37.3.2 FISMA requires DOT to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of

DOT; and information systems used or operated by DOT or by a contractor of DOT or other organization on behalf of DOT.

37.3.3 This Departmental Cybersecurity Policy is issued under DOT's authority to develop, document, implement, and oversee a Departmental Cybersecurity Program to provide protection for the information and information systems that support DOT's operations and assets, including those provided or managed by another Federal agency, a contractor, or other source.

37.3.4 DOT Components must comply with both the Departmental Cybersecurity Policy and the Departmental Cybersecurity Compendium. Specifically, the Departmental Cybersecurity Policy and Departmental Cybersecurity Compendium applies to:

37.3.4.1 All DOT Components and organizations conducting DOT business, operating DOT information systems, and collecting and/or maintaining information for, or on behalf of DOT;

37.3.4.2 All DOT permanent and temporary employees, consultants, contractors, interns, authorized personnel and other non-government employees using DOT information systems and information technology resources; and

37.3.4.3 Digital information, information systems and information technology supporting DOT operations and assets, including those provided or managed by another Federal agency, a contractor, or other source.

37.3.5 Conversely, this Departmental Cybersecurity Policy and the supporting Departmental Cybersecurity Compendium does NOT apply to the following:

37.3.5.1 Any network or information system that processes, stores, or transmits foreign intelligence or national security information under the cognizance of the Special Assistant to the Secretary (National Security) pursuant to Executive Order 12333, United States Intelligence Activities, or subsequent orders. The Director of Office of Intelligence, Security and Emergency Response (S-60) is the point of contact for issuing information system security policy and guidance for these systems.

37.3.5.2 Any public users of any DOT information systems.

(Table of Contents)

Section 37.4 Policy

37.4.1 The DOT Components must comply with both the Departmental Cybersecurity Policy and the Departmental Cybersecurity Compendium.

37.4.2 The DOT Components may exercise flexibility in the solutions used to meet the Government-wide mandates and baselines; however, they may not apply less restrictive directives or measures that are not compliant and/or aligned with the minimum requirements of this policy and the supporting Departmental Cybersecurity Compendium.

37.4.3 This Departmental Cybersecurity Policy and the Departmental Cybersecurity Compendium reference NIST SPs and other guidelines. When referenced, the current, final, published version of these guidelines and requirements are applicable.

37.4.4 All DOT information systems that generate, store, process, transfer, display, or communicate non-national security information and DOT information processed on DOT contractor information systems must be protected at a level commensurate with the potential impact of a loss of confidentiality, integrity, or availability on organizations' operations, assets, or individuals.

37.4.5 Each information system must be assigned an impact level using NIST's Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*. Once the impact level has been established, the corresponding cybersecurity requirements are identified using FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems* and NIST SP 800-53 *Recommended Security Controls for Federal Information Systems* as adopted by DOT in the Departmental Compendium. By doing so, DOT will provide an appropriate level of protection commensurate with the criticality and sensitivity of the information and information system and the potential impact in case of a security breach. Adherence to other NIST guidelines[1] is required in accordance with OMB[2] guidance.[3]

37.4.6 DOT Components must review the use of compensating controls, document those controls in the information System Security Plan (SSP) along with other appropriate security documentation for the information system, and request approval of those controls from the Authorizing Official (AO) or his/her designated representative (AODR) for the information system. DOT Components must employ compensating controls for information systems only under the following conditions:

37.4.6.1 Select compensating control(s) from the security control catalog in NIST SP 800-53.

37.4.6.2 Obtain approval on rationale and justification for choosing the compensating control(s) over an equivalent security capability or level of protection.

[1] http://csrc.nist.gov/index.html

[2] http://www.whitehouse.gov/omb/

[3] *FIPS are compulsory for Federal agencies. Guidance documents and recommendations are issued in the NIST SP 800-series. According to NIST: while agencies are required to follow NIST guidance in accordance with OMB policy, there is flexibility in how agencies apply the guidance, unless otherwise specified by OMB. Consequently, the application of NIST guidance by agencies can result in different security solutions that are equally acceptable, compliant with the guidance, and meet the OMB definition of adequate security for federal information systems. For more information, refer to* http://csrc.nist.gov/sec-cert/ca-compliance.html.

37.4.6.3 Accept risk associated with employing the compensating control(s) and document the acceptance in writing.

37.4.7 DOT Components must assess the effectiveness of security control implementation through assessment plans and testing in accordance with NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Systems and Organizations* and supplemental guidance specified in the Departmental Cybersecurity Compendium.

37.4.8 DOT Components must comply with the DOT's minimum requirements when preparing security authorization packages for information systems. DOT minimum content requirements for security authorization packages must be consistent with the NIST SP 800-37, *Guide for applying the Risk Management Framework to Federal Information Systems* methodology and the supplemental guidance contained in the Departmental Cybersecurity Compendium.

37.4.9 DOT Components must ensure that AOs are presented with the results of security assessment activities indicating the residual risks associated with unmitigated weaknesses and vulnerabilities. DOT Components must assist AOs in determining the acceptability of the residual risks, in accordance with DOT's risk management strategy specified in the Departmental Cybersecurity Compendium. DOT Components must ensure that Plans of Action and Milestone (POA&M) are prepared to mitigate the unacceptable risks.

37.4.10 The DOT Components must ensure that AO decisions to grant security authorization are documented in accordance with NIST SP 800-37 and supplemental policy and procedures specified in the Departmental Cybersecurity Compendium. DOT Components must report the security posture (defined as evidence of completion of the security authorization process), the security authorization and acceptance of risks, and the POA&M to the DOT Chief Information Security Officer (CISO) via the process and procedures specified in the Departmental Cybersecurity Compendium.

37.4.11 DOT systems that have attained a security authorization in accordance with the Departmental Cybersecurity Policy must immediately perform continuous monitoring to maintain the security authorization in accordance with NIST SP 800-37 and DOT supplemental policy and procedures specified in the Departmental Cybersecurity Compendium.

37.4.12 DOT Components must develop and implement a strategy for continuous monitoring of information system security controls to continually evaluate the effectiveness these controls as well as impacts to these controls from proposed or actual changes to the information system and its environment. The Departmental Cybersecurity Compendium specifies DOT's continuous monitoring strategy, which each DOT Component must align its continuous monitoring strategy, along with related policy and procedures to supplement NIST, OMB, and DHS guidance.

37.4.13 DOT Components must incorporate Departmental and any Component-specific Cybersecurity Policy, guidance, and standards into contract language and acquisition documents as appropriate.

37.4.14 As Federal requirements are developed and revised, DOT Components have one year from the date of issuance to adopt the revised requirements, develop new requirements, and/or update existing information systems to comply with the revised requirements before granting security authorizations, unless:

37.4.14.1 Specified by national regulation, OMB guidance or DOT policy.

37.4.14.2 Specified by an Executive Order.

37.4.14.3 A waiver is granted in accordance with this policy, Section 37.9, *Waivers*.

37.4.15 DOT personnel who are assigned roles and responsibilities in this policy to implement and manage the DOT Cybersecurity Program (the DOT CISO, DOT Component Information Systems Security Managers (ISSM), and Information System Security Officers (ISSO)) must meet minimum qualifications for position risk/sensitivity, education, competency, and certifications as defined by the Office of Personnel Management for their job series as well as supplemental criteria specified in the Departmental Cybersecurity Compendium, Appendix D: Specialized Security Training Program. If personnel assigned to these roles do not meet DOT established minimum criteria, the DOT Component security program or System Owner must identify this as a weakness and create, in the DOT Cybersecurity Assessment and Management (CSAM) tool, a Plan of Action and Milestone (POA&M) to report the weakness and corresponding corrective action plan.

(Table of Contents)

Section 37.5 Roles and Responsibilities

This section defines the roles key to implementing the Departmental Cybersecurity Program across DOT along with cybersecurity-specific responsibilities associated with each role. Provided below is a summary listing of the roles and the levels in the organization which they reside.

Department Level

- Secretary of Transportation
- Office of Security
- Office of Intelligence, Security, and Emergency Response
- Office of Budget and Programs/Chief Financial Officer (CFO)
- Office of Human Resource Management (OHRM)
- Office of the Senior Procurement Executive (OSPE)
- Risk Executive
- Department CIO
- Chief Information Security Officer (CISO)
- Senior Agency Official for Privacy (SAOP)
- Chief Privacy Officer

Component Level

- Component Administrators
- Component Human Resource Officers
- Component Procurement and Acquisition Officials
- Component Risk Executive
- Component Chief Information Officer (CIO)
- Component Information System Security Manager (ISSM)
- Component Chief Privacy Officer

Program Level

- Program Executives
- Project/Program Managers
- Contingency Planning Coordinators
- Contracting Officers (CO) and other authorized Federal representatives
- Contracting Officer’s Technical Representatives (COTR)

DOT-Wide

- Supervisors
- DOT Employees and Contractors

Information System Level

- Authorizing Official (AO)
- AO Designated Representative (AODR) (Optional)
- Information Owner (IO)
- System Owner (SO)
- Information System Security Officer (ISSO)
- Security Control Assessor (SCA)
- System Technical Support Staff

Special Cybersecurity Teams, Groups, and Councils

- DOT Computer Security Incident Response Center (DOT CSIRC)
- Component Computer Security Incident Response Teams (CSIRT)
- DOT Cybersecurity Steering Group

Department Level: All Department level roles must be filled by Federal Government employees.

37.5.1 The cybersecurity-related responsibilities of the **Secretary of Transportation** include, but are not limited to the following:

37.5.1.1 Ensuring a Departmental Cybersecurity Program is developed, documented, and implemented to provide security for all information systems, networks, and data that support departmental operations;

37.5.1.2 Ensuring cybersecurity management processes are integrated with DOT strategic and operational planning processes;

37.5.1.3 Ensuring the DOT Risk Executive function is delegated to a senior Government official or group that has the ability to link risk management processes at the information system level to risk management processes at the organization level;

37.5.1.4 Ensuring the provision of resources necessary to administer the Departmental Cybersecurity Program;

37.5.1.5 Protecting information systems and data by allocating the appropriate resources, including but not limited to technical, administrative, financial and human resources, commensurate with the risk and magnitude of harm posed by unauthorized access, modification, disclosure, disruption, use, and/or destruction, or as required by law;

37.5.1.6 Ensuring senior DOT officials provide the appropriate information technology (IT) security based on risk-based decisions for operations and IT resources under their control;

37.5.1.7 Designating an Assistant Secretary-level or equivalent executive to serve as the Departmental CIO with overall accountability for ensuring that DOT appropriately implements information security protections;

37.5.1.8 Delegating to the DOT CIO the authority to ensure compliance with the Departmental Cybersecurity Program;

37.5.1.9 Ensuring DOT provides necessary and adequate training to Federal personnel to support compliance with the Departmental Cybersecurity Program;

37.5.1.10 Ensuring the DOT CIO, in coordination with the DOT Component CIOs, reports annually on the effectiveness of the Departmental Cybersecurity Program and on any required remedial actions;

37.5.1.11 Establishing, through the development and implementation of policies, the organizational commitment to information security and the actions required to effectively manage risk and protect the core missions and business functions being carried out by the organization; and

37.5.1.12 Establishing appropriate accountability for information security and providing active support and oversight of monitoring and improvement for the information security program.

37.5.2 The cybersecurity-related responsibilities of the **DOT Chief Information Officer** include, but are not limited to the following:

37.5.2.1 Managing the Department's Cybersecurity Program;

37.5.2.2 Ensuring DOT compliance with Federal regulations and FISMA IT security program implementation requirements;

37.5.2.3 Requiring the development and implementation of protections for DOT information and information systems commensurate with the risk and magnitude of harm posed by unauthorized access, modification, disclosure, disruption, use, and/or destruction, or as recommended by law;

37.5.2.4 Ensuring the dissemination of Departmental Cybersecurity Policy, guidance, procedures and standards for DOT Component review and comment;

37.5.2.5 Reporting annually, in coordination with Component Heads to the Secretary of Transportation on the effectiveness of the DOT Cybersecurity Program, including progress of remedial actions;

37.5.2.6 Appointing the DOT CISO to fulfill the responsibilities of the CIO in developing and maintaining a Departmental Cybersecurity Program;

37.5.2.7 Defining and establishing the minimum security control requirements in accordance with data sensitivity and information system criticality;

37.5.2.8 Preparing any report that may be required of DOT to satisfy the reporting requirements of OMB Circular A-130 or FISMA;

37.5.2.9 Coordinating with the Secretary of Transportation to ensure the provision of necessary resources to administer and implement the Departmental Cybersecurity Program;

37.5.2.10 Providing advice and assistance to the Deputy Secretary and other senior management personnel to ensure that information resources are acquired and managed for the Department in accordance with the goals of the Capital Planning and Investment Control (CPIC) process;

37.5.2.11 Providing leadership for developing, promulgating, and enforcing agency information resource management policies, standards, and guidelines, and for procedures on data management, enterprise security performance management, enterprise security situational awareness, telecommunications, IT reviews, and other related areas;

37.5.2.12 Establishing, implementing, and enforcing a DOT-wide framework to facilitate an incident response program and ensuring proper and timely reporting to the United States Computer Emergency Readiness Team (US-CERT);

37.5.2.13 Resolving any disputes related to the development of responses to OIG reviews and audits that cannot be resolved at the Component level; providing assistance to senior organizational officials concerning their security responsibilities associated with the remediation of the findings;

37.5.2.14 Informing the CFO of any cybersecurity weaknesses that constitute significant deficiencies under FISMA for inclusion in the annual assurance letter;

37.5.2.15 Determining, based on organizational priorities, the appropriate allocation of resources dedicated to the protection of the information systems supporting the organization's missions and business functions;

37.5.2.16 Unless otherwise specified by the Secretary of Transportation, perform the role of the Department's Risk Executive.

37.5.2.17 Work closely with DOT Component Heads, Component CIOs, Component Risk Executives, Component ISSMs, and AOs for:

37.5.2.17.1 Ensuring the Departmental Cybersecurity Program is effectively implemented, resulting in adequate security for all organizational information systems and environments of operation for those information systems;

37.5.2.17.2 Ensuring information security considerations are integrated into programming/planning/budgeting cycles, enterprise architectures, and acquisition/system development life cycles;

37.5.2.17.3 Ensuring information systems are covered by approved security plans and are authorized to operate;

37.5.2.17.4 Ensuring information security-related activities required across the organization are accomplished in an efficient, cost-effective, and timely manner; and

37.5.2.17.5 Ensuring a centralized reporting process is in place to support appropriate information security-related activities.

37.5.2.18 Completing mandatory annual specialized information security training.

37.5.3 The cybersecurity-related responsibilities of the **DOT Chief Information Security Officer** include, but are not limited to:

37.5.3.1 Providing management leadership in cybersecurity policy and guidance, expert advice and collaboration among DOT Components in developing, promoting and maintaining IT security measures to adequately and cost effectively protect and ensure the confidentiality, integrity and timely availability of all data and information in the custody of the Department, as well as of the information systems required to meet the Department's current and future business needs;

37.5.3.2 Assisting and advising the DOT CIO in the development, documentation, and implementation of the Departmental Cybersecurity Program (e.g., issuing policy, maintaining situational awareness, and performing compliance oversight) in order to provide cybersecurity safeguards for the electronic information and information systems that support DOT's operations and assets, including those provided or managed by another Federal organization, a contractor, or other source;

37.5.3.3 Overseeing OCIO personnel with significant responsibilities for information security and ensuring the personnel are adequately trained;

37.5.3.4 Maintaining a comprehensive inventory of all General Support Systems (GSS) and Major Applications (MA) in use within DOT;

37.5.3.5 Ensuring all IT resources are reviewed in order to ensure compliance with established Departmental and applicable external policies, standards, and regulations;

37.5.3.6 Monitoring the Departmental Cybersecurity Program activities for DOT Components;

37.5.3.7 Fostering communication and collaboration among DOT's security stakeholders to share knowledge and better understand threats to Departmental information;

37.5.3.8 Carrying out the CIO security responsibilities under FISMA and overseeing the preparation of monthly, quarterly and annual FISMA reports;

37.5.3.9 Developing and implementing a cybersecurity performance measurement program to evaluate the effectiveness of technical and non-technical information system security safeguards used to protect DOT's information;

37.5.3.10 Coordinating requirements with the DOT Director of Security (M-40) and other responsible office(s) for personnel clearances, position sensitivity, and access to information systems;

37.5.3.11 Ensuring personnel have completed the DOT investigative requirements and are approved by DOT Director of Security (M-40) before allowing them to access DOT IT systems;

37.5.3.12 Ensuring all DOT-owned telephony equipment is provided with information system and physical protection;

37.5.3.13 Implementing a security incident monitoring program for the Department that centralizes and coordinates incident reporting. This function is called the DOT Computer Security Incident Response Center (CSIRC).

37.5.3.14 Disseminating information on potential security threats and recommended safeguards;

37.5.3.15 Ensuring, in coordination with the DOT CIO and the DOT Chief Procurement Official, that all IT acquisitions include Departmental security considerations;

37.5.3.16 Ensuring the Department-wide implementation of Federal policies and procedures related to cybersecurity;

37.5.3.17 Overseeing the DOT CSIRC and managing the resources that support DOT CSIRC operations;

37.5.3.18 Serving as the primary liaison for the CIO to DOT Component CIOs, AOs, Information System Owners, Common Control Providers, and DOT Component Information Systems Security Managers (ISSM);

37.5.3.19 Providing management and oversight of activities under IT Critical Information Protection (CIP); and

37.5.3.20 Completing mandatory annual specialized information security training.

37.5.4 The cybersecurity-related responsibilities of the **DOT Senior Agency Official for Privacy** include, but are not limited to:

37.5.4.1 Approving DOT's submission of the Privacy Management portion of the annual FISMA report;

37.5.4.2 Appointing the DOT Chief Privacy Officer.

37.5.5 The cybersecurity-related responsibilities of the **DOT Chief Privacy Officer** include, but are not limited to:

37.5.5.1 Ensuring implementation of information privacy protections, including full compliance with Federal laws, regulations, and policies relating to information privacy, such as the Privacy Act of 1974, 5 U.S.C. Section 552a (henceforth, "Privacy Act") and the E-Government Act of 2002;

37.5.5.2 Preparing DOT's submission of the Privacy Management portion of the annual FISMA report in coordination with the DOT CISO; and

37.5.5.3 Defining policy, guidance, and associated processes for the preparation, review, and approval of Privacy Threshold Analyses (PTA) and Privacy Impact Assessments (PIA) to support DOT information systems.

37.5.6 The cybersecurity-related responsibilities of the **DOT Director of Security (M40)** include, but are not limited to:

37.5.6.1 Partnering with the DOT CIO and DOT Component CIOs to develop, implement, and oversee personnel security controls for access to sensitive data and for the system administrators who operate critical systems;

37.5.6.2 Providing overall leadership for the development, coordination, application, and evaluation of all policies and activities within DOT that relate to physical and personnel security, the security of classified information, and the exchange and coordination of national security-related strategic information with other Federal agencies and the national security community including national security-related relationships with law enforcement organizations and public safety agencies;

37.5.6.3 Providing current and timely intelligence or national security information to the DOT CSIRC and any DOT Component CSIRT and other key personnel responsible for incident response and exchanging and coordinating national security-related strategic information with other Federal agencies and the national security community, including national security-related relationships with law enforcement organizations and public safety agencies;

37.5.6.4 Providing the necessary sponsorship and provision of National Security Systems to the DOT CSIRC and corresponding mechanisms such as e-mail and websites to communicate security and privacy vulnerabilities, threats, and incidents;

37.5.6.5 Assuring the integration of strategic medical, public health, biomedical, and national security information;

37.5.6.6 Advising on the requirements for the physical protection of computers, peripheral devices, systems, and storage media that process or contain classified national security information;

37.5.6.7 Assisting in identifying national Information Technology policy that must be followed for the processing and storage of classified national security information;

37.5.6.8 Approving visits by any foreign national, as appropriate, to any DOT Component or other facility designated as Critical Infrastructure in conjunction with the Director of Intelligence, Security, and Emergency Response;.

37.5.6.9 Ensuring communication security, including secure telecommunications equipment and classified information systems, for the discussion and handling of classified information in support of the detection, defense, and response to security vulnerabilities, threats, and incidents;

37.5.6.10 Protecting employees and visitors; and

37.5.6.11 Protecting Department-owned and -occupied critical infrastructure.

37.5.7 The cybersecurity-related responsibilities of the **DOT Director of Intelligence, Security, and Emergency Response (S60)** include, but are not limited to:

37.5.7.1 Providing current and timely intelligence or national security information to the DOT CSIRC, any DOT Component CSIRT, and other key personnel responsible for incident response; and

37.5.7.2 Providing the appropriate intelligence and coordination of visits by any foreign national to any DOT Component or DOT facility designated as Critical Infrastructure.

37.5.8 The cybersecurity-related responsibilities of the **DOT Chief Financial Officer** include, but are not limited to:

37.5.8.1 Coordinating DOT’s internal controls program to establish responsibility for uniform security-level designations for the financial management system according to the guidelines of OMB Circular A-127, Financial Management Systems; and

37.5.8.2 Targeting/selecting entities to be reviewed per OMB Circular A-123, *Management's Responsibility for Internal Control*, and applying risk-based, business-driven logic to maximize the effectiveness of the evaluations.

37.5.9 The cybersecurity-related responsibilities of the **DOT Director Office of Human Resource Management** include, but are not limited to:

37.5.9.1 Ensuring personnel officers notify the DOT Component ISSO, or designated Point of Contact (POC) for physical and logical access controls, of an employee's separation within one business day.

37.5.10 The cybersecurity-related responsibilities of the **DOT Director Office of the Senior Procurement Executive** include, but are not limited to:

37.5.10.1 Partnering with the DOT CIO to develop and implement IT security and privacy-related contract clauses for incorporation in all current and future contracts and covered grants;

37.5.10.2 Promoting the appropriate use of the required clauses in all applicable contracts; and

37.5.10.3 Ensuring contracting officers (COs) enforce the requirements of IT security and privacy clauses.

<u>Component Level</u>: All Component roles must be assigned to and performed by Federal Government employees.

37.5.11 The cybersecurity-related responsibilities of **DOT Component Administrators** include, but are not limited to:

37.5.11.1 Ensuring a Component Cybersecurity Program is developed within their organizations in accordance with the Departmental Cybersecurity Policy;

37.5.11.2 Ensuring the Risk Executive function for the Component is delegated to a senior Government official or group that has the ability to link risk management processes at the information system level to risk management processes at the organization level;

37.5.11.3 Ensuring AOs are appointed for all Component information systems, that the appointee is no less than a Component SES-level Government employee and that this appointment is documented and provided to the Component ISSM and DOT CISO;

37.5.11.4 Ensuring the Component practices its Cybersecurity Program throughout the life cycle of each Component information system;

37.5.11.5 Ensuring a report on the Component Cybersecurity Program and any internal annual compliance review is submitted annually to the DOT CISO;

37.5.11.6 Ensuring Component IT assets designated as CRITICAL under Homeland Security Presidential Directive (HSPD)-7 are protected at a FIPS 199 HIGH level unless a waiver is approved by the DOT CIO;

37.5.11.7 Protecting Component information systems and data by allocating the appropriate resources, including but not limited to technical, administrative, financial and human resources, commensurate with the risk and magnitude of harm posed by unauthorized access, modification, disclosure, disruption, use, and/or destruction, or as required by law;

37.5.11.8 Ensuring senior Component officials provide the appropriate IT security using risk-based decisions for operations and IT resources under their control;

37.5.11.9 Establishing appropriate accountability for information security and providing active support and oversight of monitoring and improvement for the information security program; and

37.5.11.10 Ensuring Component IT investments or programs are reviewed by the Component ISSM to ensure appropriate security requirements are included and necessary resources included in the budget.

37.5.12 The cybersecurity-related responsibilities of **Component Chief Information Officers** include, but are not limited to:

37.5.12.1 Managing the non-national security Cybersecurity Program for their Component and advising the Component head on significant issues related to the Component Cybersecurity Program;

37.5.12.2 Reporting Component cybersecurity-related information to the DOT CIO to meet the Department’s cybersecurity requirements;

37.5.12.3 Ensuring an information system inventory is maintained following the DOT FISMA inventory process defined in the Departmental Cybersecurity Compendium and that this inventory is updated at least annually or as directed by the DOT CIO;

37.5.12.4 Ensuring security assessment and authorization (formerly called certification and accreditation (C&A)) of Component information systems is accomplished in accordance with minimum security control guidelines established by DOT based on NIST FIPS 200, the NIST Risk Management Framework (RMF), and supplemental policy, procedures and standards specified in the Departmental Cybersecurity Compendium;

37.5.12.5 Ensuring the AO role is appointed and documented for each Component system;

37.5.12.6 Appointing the individual that fulfils the role of the Component ISSM and that this appointment is documented;

37.5.12.7 Ensuring the Component capability is maintained for computer scans, incident response, and reporting of security incidents via a Component CSIRT or an agreement for services with the DOT CSIRC; Ensuring that security incidents are detected and reported to the DOT CSIRC within US-CERT guidelines as supplemented by the DOT CSIRC;

37.5.12.8 Ensuring all external connections to/from Component information systems and networks are provided by an approved DOT Trusted Internet Connection Access Provider (TICAP) or DOT-approved Managed TIC Provider Service (MTIPS);

37.5.12.9 Ensuring all devices implemented to form internal trust boundaries send security event logs to the DOT CSIRC for integration and analysis;

37.5.12.10 Ensuring procedures are established to notify the appropriate Human Resource Officer or his/her designee, of all incidents reported to the DOT CSIRC that involves the compromise or loss of an information system or Personally Identifiable information (PII). The procedures should address means for identifying the supervisors of individuals involved in the incident and whether the circumstances of the incident suggest that corrective action is necessary;

37.5.12.11 Ensuring specialized cybersecurity training is provided annually to the individuals with significant information system security or Cybersecurity Program responsibilities within the Component;

37.5.12.12 Ensuring information system security awareness training is provided annually to Component employees and contractors with access to DOT information systems;

37.5.12.13 Ensuring that personnel who perform roles with significant security responsibilities within the Component complete applicable annual specialized security training as specified in the Departmental Cybersecurity Compendium;

37.5.12.14 Assisting the Department in compliance reviews, remediation of audit findings, and reporting requirements;

37.5.12.15 Ensuring weaknesses are correctly identified and appropriately prioritized within the Component security program and system POA&M submission;

37.5.12.16 Reviewing, in consultation with the appropriate AO and the Component ISSM, any requested exemptions to policy and signing approved exemptions; and

37.5.12.17 Completing mandatory annual specialized information security training.

37.5.13 The **Risk Executive function** must be assigned to an individual or group. It is an inherent government function and must be performed by Federal Government employees. The responsibilities of this individual or group include:

37.5.13.1 Providing a comprehensive, organization-wide, holistic approach for addressing risk—an approach that provides a greater understanding of the integrated operations of the organization;

37.5.13.2 Developing a risk management strategy for the organization and providing a strategic view of information security-related risks with regard to the organization as a whole;

37.5.13.3 Facilitating the sharing of risk-related information among AOs and other senior leaders within the organization;

37.5.13.4 Providing oversight for all risk management-related activities across the organization (e.g., security categorizations) to help ensure consistent and effective risk acceptance decisions; Ensuring that authorization decisions consider all factors necessary for mission and business success;

37.5.13.5 Providing an organization-wide forum to consider all sources of risk (including aggregated risk) to organizational operations and assets, individuals, other organizations, and the Nation;

37.5.13.6 Promoting cooperation and collaboration among authorizing officials to include authorization actions requiring shared responsibility;

37.5.13.7 Ensuring the Component mission/business functions using external providers of information and services receives the needed visibility and is elevated to the appropriate decision-making authorities;

37.5.13.8 Identifying the organizational risk posture based on the aggregated risk to information from the operation and use of the information systems for which the organization is responsible; and

37.5.13.9 Ensuring that individuals assigned this function or that participate as part of a group that performs this function complete mandatory annual specialized information security training.

37.5.14 The cybersecurity-related responsibilities of **Component Information Systems Security Managers (ISSM)** include, but are not limited to:

37.5.14.1 Overseeing the Component Cybersecurity Program;

37.5.14.2 Ensuring the Component CIO and DOT CISO are kept apprised of all pertinent matters involving the security of information systems;

37.5.14.3 Ensuring information security-related decisions and information, including updates to this Departmental Cybersecurity Policy and the supplemental Departmental Cybersecurity Compendium, are distributed to the ISSOs and other appropriate persons within their Component;

37.5.14.4 Ensuring DOT guidance is followed to identify, categorize and report an accurate information systems inventory for the Component and that this inventory is reported and maintained in accordance with DOT policy and guidance contained within the Departmental Cybersecurity Compendium;

37.5.14.5 Validating all Component information system security reporting;

37.5.14.6 Managing information security resources including oversight and review of security requirements in funding documents;

37.5.14.7 Testing, periodically, the security of implemented information systems;

37.5.14.8 Implementing and managing a POA&M process for remediation;

37.5.14.9 Serving as the primary liaison for the Component CIO to the Component's AOs, information system owners, common control providers, and ISSOs;

37.5.14.10 Ensuring each system has an ISSO appointed by the Component and that this appointment is documented;

37.5.14.11 Ensuring weekly incident reports are forwarded to the DOT CISO;

37.5.14.12 Acknowledging receipt of alerts, advisories, and bulletins sent by the DOT CSIRC and ensuring these messages are routed to the appropriate Component personnel;

37.5.14.13 Providing the DOT CSIRC the current list of Component personnel that are authorized to interact with the DOT CSIRC to include, at a minimum, the Component CIO, Component ISSM and Component ISSOs;

37.5.14.14 Ensuring adherence to DOT-approved Secure Configuration Baselines defined in the Departmental Cybersecurity Compendium;

37.5.14.15 Developing and publishing procedures necessary to implement the requirements of DOT information security policy within the appropriate Component;

37.5.14.16 Implementing Departmental information security policies, procedures, and control techniques to address all applicable requirements;

37.5.14.17 Ensuring personnel with significant responsibilities for cybersecurity are identified as specified in the Departmental Cybersecurity Compendium and that annual training is completed, tracked, and reported;

37.5.14.18 Leading Component cybersecurity and incident response programs;

37.5.14.19 Promoting proper Cybersecurity practices;

37.5.14.20 Supporting the DOT CISO in the implementation of the DOT Cybersecurity Program;

37.5.14.21 Fostering communication and collaboration among DOT security stakeholders to share knowledge and to better understand threats to DOT information;

37.5.14.22 Providing information about the Component cybersecurity policies to management and throughout DOT;

37.5.14.23 Providing advice and assistance to other organizational personnel concerning the security of sensitive data and of critical data processing capabilities;

37.5.14.24 Advising the Component CIO about security breaches in accordance with the security breach reporting procedures developed and implemented by the DOT Component;

37.5.14.25 Disseminating information on potential security threats and recommended safeguards;

37.5.14.26 Ensuring roles with significant security responsibilities are identified and documented per the Departmental Cybersecurity Compendium;

37.5.14.27 Conducting security education and awareness training needs assessments to determine requirements and leveraging available DOT-wide resources to satisfy these requirements. When DOT-wide available resources do not meet requirements, coordinating with Component CIO and Component program officials to identify cost effective solutions for meeting mandatory requirements in accordance with DOT awareness and training policy specified in the Departmental Cybersecurity Compendium;

37.5.14.28 Providing feedback obtained from Component users of DOT-wide training resources to the DOT CISO to aid in improving the content and delivery of DOT-provided training;

37.5.14.29 Assisting System Owners in establishing and implementing the required security safeguards to protect computer hardware, software, and data from improper use or abuse;

37.5.14.30 Communicating requirements for personnel clearances and position sensitivity determinations necessary for access to information systems with the appropriate office;

37.5.14.31 Ensuring Component-wide implementation of DOT and Component policies and procedures that relate to Cybersecurity and incident response;

37.5.14.32 Collaborating with the DOT Privacy Breach Response Team (BRT) Coordinator when engaging the Component POC for information collection and clarification, and sitting on the DOT Privacy BRT while the breach is under investigation;

37.5.14.33 Immediately notifying the Component Privacy Officer and DOT Privacy Officer when privacy-related or PII incidents are suspected or reported within the Component;

37.5.14.34 Establishing, documenting, and enforcing requirements and processes for granting and terminating all administrative privileges including, but not limited to, servers, domains, and local workstations auditing these processes for effectiveness in accordance with policy specified in the Departmental Cybersecurity Compendium;

37.5.14.35 Ensuring enterprise security tools are leveraged to their fullest extent and ensuring all security tools that the Component selects and implements conforms to the DOT Cybersecurity continuous monitoring technical architecture and standards;

37.5.14.36 Ensuring Component incidents are reported to the DOT CSIRC in accordance with DOT Cybersecurity policies and DOT CSIRC procedures; and

37.5.14.37 Completing mandatory annual specialized information security training.

37.5.15 The cybersecurity-related responsibilities of **Component Privacy Officer** include, but are not limited to:

37.5.15.1 Meeting the reporting requirements outlined in OMB M-08-21, FY 2008 (or its successors) *Reporting Instructions for the Federal Information Security Management Act* and Agency Privacy Management; and

Developing the Component Privacy Management portion of DOT's FISMA Report and submitting this report to the DOT Privacy Officer.

37.5.16 The cybersecurity-related responsibilities of **Component Human Resource Officer** include, but are not limited to:

37.5.16.1 Coordinating with appropriate Component POCs and servicing security organization (SSO) POCs to ensure background checks are conducted for individuals with significant security responsibilities;

37.5.16.2 Notifying the appropriate Component POC within 1 business day when Component personnel are separated from the Department and notifying the SSO POC when personnel are separated from the Department;

37.5.16.3 Ensuring relevant paperwork, interviews, and notifications are sent to the appropriate Component CIO personnel when employees join, transfer within, or leave the organization, either permanently or on detail and notifying the SSO POC when personnel are separated from the Department;

37.5.16.4 Participating at the request of the DOT CSIRC in the investigation of Federal employees with regard to security incidents;

37.5.16.5 Participating at the request of the DOT Privacy BRT in the investigation of Federal employees relative to PII incidents and violations;

37.5.16.6 Reporting actual or suspected computer-security incidents including PII breaches to the DOT CSIRC within timeframes established by DOT Incident Response policy for incident types in accordance with US-CERT; and

37.5.16.7 Reporting actual or suspected privacy-related incidents including PII breaches to the DOT Privacy Officer and the Component Privacy Officer immediately.

37.5.17 The cybersecurity-related responsibilities of **Component Procurement and Acquisition Officials** include, but are not limited to:

37.5.17.1 Ensuring cybersecurity is addressed in all IT procurements and other procurements as appropriate; and

37.5.17.2 Ensuring contract vehicles address mandatory Federal and Departmental security requirements.

Program Level - Program level roles apply to all DOT Components.

37.5.18 The cybersecurity-related responsibilities of **Program Executives,** who must be Federal Government employees**,**[4] include, but are not limited to:

37.5.18.1 Ensuring information systems and data that are critical to the Program's mission receive adequate protection;

37.5.18.2 Determining, in coordination with the Data Owner/Business Owner and System Owner, appropriate security controls and identifying resources to implement those controls; and

37.5.18.3 Ensuring security for each information system is planned, documented, and integrated into the System Development Life Cycle (SDLC) from the information system's initiation phase to the system's disposal phase. At DOT, the SDLC is implemented as the Integrated Program Planning and Management (IPPM) program.

37.5.19 The **Contingency Planning Coordinators** coordinate contingency planning strategy across DOT Components. This role has been placed at the "program level" to permit DOT Components to assign the role to Government or contractor personnel as well as permit DOT Components to assign the role based on the needs of each organization. At a minimum, each DOT Component must have at least one individual assigned to fulfill the duties of this role for their respective organization. The cybersecurity-related responsibilities include, but are not limited to:

37.5.19.1 Developing the contingency plan (CP) strategy, in cooperation with other functional and resource managers associated with the DOT Component or the business processes supported by the organization;

37.5.19.2 Coordinating with other offices and personnel that are responsible for the development and management of DOT and Component Business Continuity Plans (BCP), Continuity of Operations (COOP) Plans, Crisis Communications Plans, Critical Infrastructure Protection (CIP) Plans, Cyber Incident Response Plans, and Disaster Recovery Plans (DRP) to ensure the necessary exchange of information relevant to information system(s) assigned responsibility;

37.5.19.3 Coordinating with the ISSOs and other key functional and resource managers

[4] In some cases, the Program Executive may be the System Owner and/or the Information Owner.

in the Department and/or Component to test Information System Contingency Plans (ISCP) in accordance with policy and standards defined in the Departmental Cybersecurity Compendium;

37.5.19.4 Ensuring each team is trained and ready to deploy in the event of a disruptive situation requiring CP activation;

37.5.19.5 Ensuring recovery personnel are assigned to each team to respond to the event, recover capabilities, and return the system to normal operations; and

37.5.19.6 Reporting actual or suspected computer-security incidents including PII breaches to the DOT CSIRC within timeframes established by DOT Incident Response policy for incident types in accordance with US-CERT.

37.5.20 The cybersecurity-related responsibilities of **Contract Officers (CO) and other authorized Federal representatives,** who must be Federal Government employees, include, but are not limited to:

37.5.20.1 Coordinating with the System Owner, Data Owners/Business Owners, Project Officer/Manager, and CISO to ensure that the appropriate security contracting language from DOT Chief Procurement Officer and other relevant sources are incorporated into each IT contract;

37.5.20.2 Advising contractors that develop or maintain a Privacy Act System of Records (SOR) on behalf of the Federal Government that the Privacy Act applies to them to the same extent that it applies to the government, per subsection (m) of the Privacy Act;

37.5.20.3 Maintaining the integrity and quality of the proposal evaluation, negotiation, and source selection processes, while ensuring all terms and conditions of the IT contract are met;

37.5.20.4 Monitoring contract performance and reviewing deliverables for conformance with contract requirements related to cybersecurity;

37.5.20.5 Taking action as needed to ensure that accepted products meet contract requirements;

37.5.20.6 Ensuring sufficient funds are available for obligation per the Federal Acquisition Regulations (FAR);

37.5.20.7 Maintaining the integrity and quality of the proposal evaluation, negotiation, and source selection processes while ensuring all cybersecurity conditions of the contract are met;

37.5.20.8 Determining the applicability of the Privacy Act with assistance from the DOT Component Privacy Office and Component Office of Chief Counsel when the design, development, or operation of a Privacy Act SOR on individuals is required to accomplish an agency function;

37.5.20.9 Reporting actual or suspected computer-security incidents including PII breaches to the DOT CSIRC within time frames established by DOT Incident Response policy for incident types in accordance with US-CERT;

37.5.20.10 Reporting actual or suspected privacy-related incidents including PII breaches to the DOT Privacy Officer and Component Privacy Officer within time frames established by the DOT Privacy Officer; and

37.5.20.11 Completing mandatory annual specialized information security training.

37.5.21 The cybersecurity-related responsibilities of **Contracting Officer's Technical Representatives** , who must be Federal Government employees, include, but are not limited to:

37.5.21.1 Determining whether contractors require IT access to accomplish the DOT mission;

37.5.21.2 Sponsoring contract employees for a PIV card, or other appropriate identification media, and notifying the SSO when the PIV card, or other identification media, are no longer required by the employee;

37.5.21.3 Ensuring contractors comply with this policy and pursuing appropriate action for noncompliance;

37.5.21.4 Reviewing and authorizing access privileges for contractors and reviewing user security agreements at least annually (or as specified by Departmental Cybersecurity Compendium) to verify the continuing need for access, the appropriate level of privileges, and the accuracy of information contained in the agreement (e.g., information systems authorized for access and type) and subsequently providing the list of authorized personnel to the ISSM;

37.5.21.5 Notifying System Owners, within the time frames specified in the Departmental Cybersecurity Compendium, to revoke access privileges when a contractor under his/her supervision or oversight no longer requires access privileges, requires a change in access privileges, or fails to comply with stated policies or procedures;

37.5.21.6 Ensuring contractor personnel who are assigned to a DOT project with access to DOT information or information systems complete annual security awareness training and that evidence of completion is obtained and provided to the appropriate ISSO or ISSM;

37.5.21.7 Ensuring contractor personnel who are assigned a role deemed to require specialized security training complete the required level of appropriate specialized security training annually and that evidence of completion is obtained and provided to the ISSO; and

37.5.21.8 Completing mandatory annual specialized information security training.

37.5.22 The cybersecurity-related responsibilities of **Project/Program Managers**, who may be either Federal Government employees or DOT contractors, include, but are not limited to:

37.5.22.1 Evaluating proposals, if requested with the assistance of the Component ISSM and/or Component CIO, to determine whether proposed security solutions effectively address agency requirements as detailed in acquisition documents;

37.5.22.2 Ensuring security-related documentation at each phase of the SDLC meets all identified security needs; and

37.5.22.3 Reporting actual or suspected computer-security incidents including PII breaches to the DOT CSIRC within time frames established by DOT Incident Response policy for incident types in accordance with US-CERT and as appropriate report incident to CO/COTR.

DOT-wide Level – These roles apply to all DOT Components.

37.5.23 The cybersecurity-related responsibilities of **Supervisors**, who must be Federal Government employees, include, but are not limited to:

37.5.23.1 Ensuring compliance with cybersecurity policies by all personnel under their direction; and providing the personnel, financial, and physical resources required to protect information resources appropriately;

37.5.23.2 Budgeting resources for cybersecurity training and role-based training for personnel with security-related responsibilities (e.g., time, money, staff coverage);

37.5.23.3 Ensuring personnel under their direct report complete all required cybersecurity training, including role-based training, within the mandated timeframe;

37.5.23.4 Notifying the ISSO or ISSM and the SSO immediately of an unfriendly departure or separation of a DOT employee or contractor;

37.5.23.5 Following DOT and/or Component specific departure/separation checkout procedures to ensure the appropriate steps and processing are performed;

37.5.23.6 Pursuing disciplinary or adverse actions against personnel who violate DOT policies or standards, including the DOT Rules of Behavior (RoB) and Component/ -specific policies and procedures, including information system-specific RoB;

37.5.23.7 Ensuring disclosures of PII comply with the requirements of the applicable Privacy Act SOR and seeking the guidance of the Component Privacy Officer or DOT Privacy Officer and Office of General Counsel as appropriate;

37.5.23.8 Reporting actual or suspected computer-security incidents including PII breaches to the DOT CSIRC within time frames established by DOT Incident Response policy for incident types in accordance with US-CERT ;

37.5.23.9 Determining access requirements for Federal employees and contractors who report to them based on assigned job functions and communicating these requirements to System Owners and ISSOs;

37.5.23.10 Authorizing privileges for personnel and reviewing user security agreements at least annually to verify the continuing need for access, the appropriate level of privileges, and the accuracy of information contained in the agreement (e.g., information systems authorized for access and type); and

37.5.23.11 Notifying System Owners to revoke access privileges in a timely manner when a user under his/her supervision or oversight no longer requires access privileges, requires a change in access privileges, or fails to comply with stated policies or procedures, and informing the SSO when access privileges are revoked.

37.5.24 The cybersecurity-related responsibilities of all **DOT Employees and DOT Contractors** operating on behalf of DOT include, but are not limited to:

37.5.24.1 Complying with the Department's policies, standards, and procedures;

37.5.24.2 Possessing awareness that they are not acting in an official capacity when using Departmental IT resources for non-governmental purposes;

37.5.24.3 Familiarizing themselves with any special requirements for accessing, protecting, and using data, including PII, copyright data, and procurement-sensitive data;

37.5.24.4 Seeking guidance from Supervisors, ISSO or Component ISSM when in doubt about implementing this document;

37.5.24.5 Ensuring all media containing Departmental data is appropriately marked and labeled to indicate the sensitivity of the data;

37.5.24.6 Abstaining from loading unapproved software from unauthorized sources;

37.5.24.7 Ensuring sensitive data is not stored on laptop computers or other portable devices unless the data is secured using encryption standards commensurate with the sensitivity level of the data on DOT information systems or networks;

37.5.24.8 Reading, acknowledging, signing, and complying with the DOT RoB, as well as any Component-specific and/or and information system-specific RoB, before gaining access to DOT information systems and networks;

37.5.24.9 Completing required annual security awareness training;

37.5.24.10 Implementing specified security safeguards to prevent fraud, waste, or abuse of the information systems, networks, and data they are authorized to use;

37.5.24.11 Conforming to security policies and procedures that minimize the risk to DOT information systems, networks, and data from malicious software and intrusions;

37.5.24.12 Agreeing not to disable, remove, install with intent to bypass, or otherwise alter security or administrative settings designed to protect DOT IT resources;

37.5.24.13 Ensuring adequate protection is maintained on their workstations, including not sharing passwords with any other individual, and logging out, locking, or enabling a password-protected screen saver before leaving their workstation; and

37.5.24.14 Reporting actual or suspected computer-security incidents including PII breaches to the DOT CSIRC within time frames established by DOT Incident Response policy for incident types in accordance with US-CERT.

Information System Level - System level roles apply to all DOT Components.

37.5.25 The cybersecurity-related responsibilities of **Authorizing Officials**, who must be Senior Executive Service–level Government employees (previously called Designated Accrediting Authorities (DAA) and accrediting officials) include, but are not limited to:

37.5.25.1 Relying on the assistance and advice of the ISSO, System Owner, Risk Executive and ISSM, authorize operation of the relevant information system(s), including recognizing and accepting remaining residual risk, and being accountable for information system security;

37.5.25.2 Determining the acceptable level of risk and appropriate level of security and granting the approval to operate (ATO) an information system/application at a specified risk level;

37.5.25.3 Working with the Component CIO and other officials to determine the risks and associated vulnerabilities resulting from interconnecting with other programs and information systems over which the AOs have little or no control;

37.5.25.4 Appointing the individual to perform the System Owner role for the information system and ensuring that this appointment is documented and provided to the ISSM;

37.5.25.5 Appointing the individual to perform the Information Owner role for the information system or fulfilling this role directly; ensuring that this appointment is documented and provided to the ISSM;

37.5.25.6 Reviewing the security of each DOT information system under their purview in accordance with DOT continuous monitoring policy and strategy to approve the information system for continued operation;

37.5.25.7 Ensuring vulnerabilities and weaknesses associated with unacceptable risks are listed in the information system POA&M, which is updated quarterly. For POA&M items that require resources, the AO must specify whether funds will come from a reallocation of base resources or a request for new funding. If a request for new funding is deemed necessary, the AO must provide the Component CIO and DOT CIO a brief rationale to support the request;

37.5.25.8 Reviewing, in consultation with the CIO and ISSM, any requested exemptions to policy, and signing approved exemptions;

37.5.25.9 Ensuring that an ISSO has been appointed for the information system and that this individual is responsible for ensuring the security of the information system and that the information system is in compliance with information security requirements throughout the SDLC (from design through disposal);

37.5.25.10 Overseeing the budget and business operations of the information system(s) under their purview and, as called upon to do so, approving information system security requirements, system security plans, memorandums of agreement (MOA), memorandums of understanding (MOUs), and interconnection security agreements (ISAs);

37.5.25.11 In consultation with ISSM and the System Owner, determining the required level of Security Control Assessor (SCA) independence. When the assessment is conducted in support of an authorization decision or ongoing authorization, as in continuous monitoring, the AO must make an explicit determination of the degree of independence required in accordance with OMB guidance, NIST standards and DOT policies specified in the Departmental Cybersecurity Compendium;

37.5.25.12 Approving, only with concurrence of the Security Control Assessor, the use of any compensating controls for Department-wide controls, consistent with DOT policy, and ensuring such use and approval is documented and the ISSM is notified;

37.5.25.13 Retaining responsibility for the information under their purview even when the information is shared with other organizations;

37.5.25.14 Terminating information system operations if security conditions warrant such action;

37.5.25.15 Designating a representative, if desired, called the Authorizing Official Designated Representative (AODR), and empowering this individual to make certain decisions with regard to the planning and resourcing of the security management responsibilities and activities, the acceptance of the system security plan, and the determination of risk to agency operations, agency assets, and individuals. The AO may not delegate the determination of risk acceptance or security authorization decisions.

37.5.25.16 Completing mandatory annual specialized information security training.

37.5.26 The cybersecurity-related responsibilities of **System Owners (SO),** who must be a Federal Government employee, include, but are not limited to:

37.5.26.1 Procuring, developing, integrating, modifying, or operating and maintaining the DOT information system and relying on the assistance and advice of the ISSO, information system operators, and other IT staff in the implementation of security responsibilities;

37.5.26.2 Ensuring the information system is operated according to applicable security standards;

37.5.26.3 Ensuring an ISSO is appointed for the information system and that this appointment is documented and provided to the ISSM;

37.5.26.4 Ensuring information System Technical Support Staff are properly designated, monitored, and trained;

37.5.26.5 Deciding who has access to the information system and with what rights and privileges and granting individuals the fewest possible privileges necessary for job performance so that privileges are based on a legitimate need; re-evaluating access privileges annually and revoking access in a timely manner upon personnel transfer or termination, ,which may be delegated to the ISSO or other operational security personnel;

37.5.26.6 Ensuring users and support personnel receive the requisite security training;

37.5.26.7 Ensuring key organizational officials are informed of the requirement for cybersecurity to be built into DOT information systems to include minimum security control implementation, security assessment and authorization, and requirements for continuous monitoring of security controls;

37.5.26.8 Providing necessary information system-related documentation to the Security Control Assessor;

37.5.26.9 Establishing information system-level POA&Ms and implementing corrective actions in accordance with the DOT policy and procedures established for POA&Ms. This includes taking appropriate steps to update the risk assessment and to reduce or eliminate vulnerabilities after receiving the security assessment results from the Security Control Assessor;

37.5.26.10 Ensuring security assessment, authorization, and continuous monitoring of the information system, including:

37.5.26.10.1 Ensuring the security of data and application software residing on the information system;

37.5.26.10.2 Categorizing the criticality/sensitivity of the information system in accordance with FIPS 199 and ensuring the categorization receives the approval of AO;

37.5.26.10.3 Implementing a level of security commensurate with the information system impact level;

37.5.26.10.4 Developing and maintaining the Security Authorization Package as defined in the Departmental Cybersecurity Compendium;

37.5.26.10.5 Ensuring the Security Authorization Package and evidence of continuous monitoring is maintained by the organization;

37.5.26.10.6 Including security considerations and identify associated security funding requirements in the procurement of information system software, hardware, and support services, including information system development, implementation, operation and maintenance, disposal activities (i.e., life cycle management), and weakness remediation / mitigation associated with unacceptable risks tracked in POA&M;

37.5.26.10.7 Establishing appropriate rules of behavior that apply to all personnel managing, administering, or having access to the information system;

37.5.26.10.8 Reporting actual or suspected computer-security incidents including PII breaches to the DOT CSIRC within time frames established by DOT Incident Response policy for incident types in accordance with US-CERT;

37.5.26.10.9 Providing necessary assistance to DOT personnel in the investigation of security incidents;

37.5.26.10.10 Ensuring the minimum security requirements for the information system are met in accordance with FIPS 200; and

37.5.26.10.11 Ensuring NISTSP 800-53 baseline security controls (as augmented with DOT and any Component-wide supplemental policy and controls) are scoped and tailored in accordance with these guidelines and that scoping and tailoring decisions are effectively documented.

37.5.26.11 Ensuring settings are selected from the Departmental Cybersecurity Compendium for NIST SP 800-53 organizational parameterized controls and that those settings required to be set by the DOT Component are implemented in accordance with DOT Component policy;

37.5.26.12 Ensuring service providers (to include providers of contingency services) and/or operators of information systems upon which their information systems rely are informed as to the information system’s FIPS 199 impact level, augmentations to the applicable security control baseline, and the applicable security control parameters;

37.5.26.13 In the case of outsourced information systems and information technology-related services, ensuring the appropriate and applicable security controls are integrated into the procurement (or other contract or service provisioning) vehicle; and

37.5.26.14 Completing mandatory annual specialized information security training.

37.5.27 **Information Owners (IO)** are Federal Government employees/officials with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. The owner of the information stored within, processed by, or transmitted by an information system can also be the Authorizing Official. However, a single information system may utilize information from multiple Information Owners. The cybersecurity-related responsibilities of the Information Owners, as applied to the information designated under their purview include, but are not limited to:

37.5.27.1 Establishing the rules for appropriate use and protection of the subject

/information (e.g., rules of behavior);[5]

37.5.27.2 Deciding who has access to the information system and with what types of privileges or access rights;

37.5.27.3 Providing input to System Owners regarding the security requirements and security controls for the information system(s) where the information resides;

37.5.27.4 Assisting in the identification and assessment of the common security controls where the information resides;

37.5.27.5 Completing mandatory annual specialized information security training; and

37.5.27.6 Allowing production data to be stored or processed only on accredited information systems.

37.5.28 An **Information System Security Officer** (ISSO) must be appointed for each information system. An individual may serve as the ISSO for more than one system. ISSOs may be either Federal Government employees or DOT contractors. The cybersecurity responsibilities of an ISSO, as applied to each information system under their purview, include but are not limited to:

37.5.28.1 Ensuring that applicable cybersecurity policies are implemented for the information system and for those aspects of information system-related physical security also under their purview;

37.5.28.2 Ensuring operational security posture consistent with current security policy is maintained;

37.5.28.3 Reporting actual or suspected computer-security incidents including PII breaches to the DOT CSIRC within time frames established by DOT Incident Response policy for incident types in accordance with US-CERT;

37.5.28.4 Ensuring cybersecurity notices and advisories are distributed to appropriate personnel and that vendor-issued security patches are expeditiously installed;

37.5.28.5 Serving as the primary liaison for security matters for the AO to information system owners, common control providers, and users;

37.5.28.6 Serving as an focal point for cybersecurity incident reporting and subsequent resolution for assigned information systems;

[5] The Information Owner retains this responsibility even when the data/information is shared with other organizations.

37.5.28.7 Assisting the ISSM in reviewing contracts for information systems under the Component's control to ensure that cybersecurity is appropriately addressed in contract language;

37.5.28.8 Ensuring security-related documentation at each phase of the SDLC meets all identified security needs;

37.5.28.9 Maintaining the security assessment and authorization documentation (formerly called C&A) for information systems under his or her purview, according to Departmental Cybersecurity Policy and Compendium;

37.5.28.10 Ensuring the selection of NIST SP 800-53 baseline security controls are appropriate for the information system based on the FIPS 199 security categorization, NIST SP 800-53 guidance, and supplemental DOT policy specified in the Departmental Cybersecurity Compendium;

37.5.28.11 Assisting the System Owner, Information Owner, and ISSM in recording all known security weaknesses of assigned information systems in the POA&M in accordance with DOT policy and procedures;

37.5.28.12 Ensuring no single individual has control of any critical process in its entirety per NIST SP 800-53 by implementing separation of duties;

37.5.28.13 Tracking all security education and awareness training conducted for personnel and contractors, as required by Departmental Cybersecurity Policy and Compendium;

37.5.28.14 Providing security advice to the AO and System Owner on all matters (technical and otherwise) involving security of the information system;

37.5.28.15 Ensuring required updates are performed to key documents in accordance with NIST SP 800-37 for continuous monitoring as supplemented by Departmental Cybersecurity Policy and Compendium;

37.5.28.16 Identifying changes to the information system that may impact security controls, performing the security impact assessment of proposed changes, reporting any change in risk posture, and providing recommendations for risk mitigation;

37.5.28.17 Ensuring proper backup procedures exist for assigned information systems and that procedures are performed and tested in accordance with the System Security Plan;

37.5.28.18 Assisting the System Owner and ISSM to ensure that external connections to/from DOT information systems and networks are provided by an approved DOT Trusted Internet Connection Access Provider (TICAP) or DOT-approved Managed TIC Provider Service (MTIPS).

37.5.28.19 Ensuring audit logs are captured, maintained, and analyzed as required by NIST SP 800-53 and any supplemental Departmental Cybersecurity Policy and the Compendium;

37.5.28.20 Ensuring the DOT enterprise information security management system (CSAM or its successors) accurately contains required information system inventory, categorization, POA&Ms and other security metrics required by the DOT CIO through this policy and the Departmental Cybersecurity Compendium for the system(s) for which the ISSO is responsible; and

37.5.28.21 Completing mandatory annual specialized information security training.

37.5.29 **Security Control Assessor (**formerly called Certification Officials and Certification Agents (CA)) may be Federal Government employees or DOT contractor individuals, groups, or organizations responsible for conducting an independent and impartial security assessment[6]. Independent security assessment services can be obtained from other elements within the organization or can be contracted to a public or private sector entity outside of the organization. Contracted assessment services are considered independent if the information system owner is not directly involved in the contracting process or cannot unduly influence the impartiality of the assessor or assessment team conducting the assessment of the security controls in the information system. These individuals must be U.S. Citizens or permanent lawful resident aliens. The cybersecurity-related responsibilities of the SCA, as they are applied to information systems and networks under his or her authority, include, but are not limited to:

37.5.29.1 Conducting a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an information system to determine the overall effectiveness of the controls (i.e., the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system);

37.5.29.2 Providing an assessment of the severity of weaknesses or deficiencies discovered in the information system and its environment of operation and recommend corrective actions to address identified vulnerabilities;

37.5.29.3 Identifying any potential conflicts of interest and notifying the AO and ISSM of situations that may impact the independence of the SCA to conduct the assessment prior to initiating the SCA;

37.5.29.4 Conducting assessment of the security plan to determine if the plan provides a set of security controls for the information system that meet the stated security requirements prior to initiating the SCA;

37.5.29.5 Ensuring the DOT security assessment and authorization process is conducted

[6] *NIST SP 800-53 CA-2 Enhancement 1 specifies that assessors be free from any perceived or actual conflicts of interest with respect to the developmental, operational, and/or management chain associated with the information system to the determination of security control effectiveness.*

in accordance with NIST guidance and the Departmental Cybersecurity Compendium;

37.5.29.6 Reviewing the information system security documentation and results of the security control assessments and providing the results of the security control assessment (the security assessment report (SAR)) in writing to the AO or AODR;

37.5.29.7 Providing an assessment of the severity of weaknesses or deficiencies discovered in the information system and its environment of operation and recommend corrective actions to address identified vulnerabilities;

37.5.29.8 Preparing the final SAR containing the results and findings from the assessment;

37.5.29.9 Assisting in the determination of risks associated with the results/findings from the assessment;

37.5.29.10 Providing recommendations to the AO regarding risk acceptance, authorization to operate, and corrective actions for POA&Ms; and

37.5.29.11 Conducting ongoing independent control assessments to support information system security continuous monitoring.

37.5.30 **System Technical Support Staff** are either Federal Government employees or DOT contractors that perform technical tasks to support the information system through its lifecycle processes (planning, development, testing, operations, decommission). These individuals frequently have special privileges that grant them greater access or control than general users. These individuals often also have access to the sensitive data contained within DOT information systems. Titles for personnel that perform in this capacity include System Administrator, Network Administrator, Database Administrator, System Engineer, Application Developer, System Tester, Security Analyst, Incident Handler and Help Desk Analyst. The cybersecurity-related responsibilities of System Technical Support Staff who may be either Federal Government employees or DOT contractors include, but are not limited to:

37.5.30.1 Reading, acknowledging, signing, and complying with the DOT information system Rules of Behavior For Use of Technology Resources and Information (DOT RoB), and Component and information system-specific RoB, before gaining access to the Department’s information systems and networks;

37.5.30.2 Completing required security awareness training;

37.5.30.3 Participating in DOT-required specialized security training;

37.5.30.4 Ensuring the cybersecurity posture of the information system, application, and network is maintained during all maintenance, monitoring activities, installations or upgrades, and throughout day-to-day operations;

37.5.30.5 Ensuring appropriate security requirements are implemented and enforced for all DOT information systems or networks;

37.5.30.6 Examining unresolved information system vulnerabilities and determining which corrective action(s) or additional safeguards are necessary to mitigate them;

37.5.30.7 Implementing proper information system backups, applying software patches within timeframes established by the DOT Component for security vulnerabilities, and accurately reporting security incidences in accordance with DOT policy, DOT CSIRC procedures, and any DOT Component supplemental procedures;

37.5.30.8 Utilizing his or her "root" or "administrative" access rights to a computer, based on need-to-know and in accordance with DOT policies defined herein and in the Departmental Cybersecurity Compendium, to include not using root, administrative, or other privileged accounts to access the internet;

37.5.30.9 Identifying to the ISSO any external connections to/from DOT information systems and networks that are not provided by an approved DOT Trusted Internet Connection Access Provider (TICAP) or DOT approved Managed TIC Provider Service (MTIPS).;

37.5.30.10 Conducting tests of security safeguards in accordance with the established test plan and procedures;

37.5.30.11 Identifying cybersecurity impacts associated with information system implementation procedures;

37.5.30.12 Leading the design, development, and modification of safeguards to correct vulnerabilities identified during information system implementation;

37.5.30.13 Recognizing potential security violations and taking appropriate action to report any such incident as required by Federal regulation, and mitigating any adverse impact;

37.5.30.14 Developing and/or executing a information system termination plan to ensure that cybersecurity breaches are avoided during shutdown, and that long-term protection of archived resources is achieved;

37.5.30.15 Ensuring hardware, software, data, and facility resources are archived, sanitized, or disposed of in a manner consistent with the information system termination plan;

37.5.30.16 Reporting actual or suspected computer-security incidents including PII breaches to the DOT CSIRC within time frames established by DOT Incident Response policy for incident types in accordance with US-CERT; and

37.5.30.17 Completing mandatory annual specialized information security training.

Special Cybersecurity Teams, Groups, and Councils

37.5.31 The cybersecurity-related responsibilities of the **DOT Computer Security Incident Response Center** include, but are not limited to:

37.5.31.1 Establishing and maintaining a partnership with all DOT security program personnel, and DOT Component CSIRTs when applicable, to ensure the DOT CSIRC is aware of security vulnerabilities, threats, and incidents that may negatively impact the ability of the Component and/or the Department to fulfill its mission and functions;

37.5.31.2 Serving as the primary entity in the Department responsible for maintaining Department-wide security incident handling, response and reporting;

37.5.31.3 Serving as the primary entity in the Department responsible for maintaining Department-wide operational cybersecurity situational awareness and determining the overall cybersecurity risk posture of DOT;

37.5.31.4 Serving as the lead organization for coordinating Departmental cybersecurity information sharing, analysis, and response activities;

37.5.31.5 Reporting DOT cybersecurity incidents to US-CERT, US DOT Crisis Management Center (CMC), and the DOT OIG;

37.5.31.6 Immediately reporting DOT privacy-related incidents to the DOT Privacy Officer and the Component Privacy Officer associated with the incident;

37.5.31.7 Serving as the Department's primary point of contact with US-CERT;

37.5.31.8 Serving as the central reporting office for cybersecurity-related incidents which may require law enforcement actions and subsequently coordinating with the DOT OIG and Component for incidents involving law enforcement action;

37.5.31.9 Performing network discovery, network security monitoring, vulnerability scanning, and penetration testing of all DOT networks; and

37.5.31.10 Performing cyber intelligence analysis and digital media analysis to support incident investigation.

37.5.31.11 Personnel that perform duties to support the DOT CSIRC must complete mandatory annual specialized information security training.

37.5.32 The cybersecurity-related responsibilities of the **Component Computer Security Incident Response Teams**[7] (CSIRT) include, but are not limited to:

37.5.32.1 Serving as the primary entity in the Component responsible for maintaining Component-wide operational cybersecurity situational awareness and determining the overall cybersecurity risk posture of the Component;

[7] *DOT OCIO encourages all DOT Components to obtain CSIRT services from the DOT CSIRC through execution of an appropriate agreement*.

37.5.32.2 Serving as the lead organization for coordinating Component-wide cybersecurity information sharing, analysis, and response activities;

37.5.32.3 Reporting Component cybersecurity-related incidents to the DOT CSIRC; and

37.5.32.4 Serving as the Component's primary point of contact with DOT CSIRC.

37.5.32.5 Personnel that perform duties to support the CSIRT must complete mandatory annual specialized information security training.

37.5.33 The cybersecurity-related responsibilities of the **DOT Cybersecurity Steering Group,** which is chaired by the DOT CISO include, but are not limited to:

37.5.33.1 Providing reviews, comments and recommendations to the DOT CIO on the initial release and subsequent updates to the Departmental Cybersecurity Compendium;

37.5.33.2 Providing reviews, comments, and recommendations to the DOT CIO on other cybersecurity policies, procedures, guidance and standards that the DOT CIO has deemed necessary to issue to address: i) Government-wide laws, regulations, guidance and standards; ii) evolving security threats, and iii) emerging information technologies;

37.5.33.3 Adhering to the guidelines that are established by the Chair for this group which will meet at least annually;

37.5.33.4 As the Chair of this group, the DOT CISO will ensure that the group’s standing members are comprised of at least one representative from the following Offices: Office of General Counsel; Assistant Secretary for Administration; Office of Security; Office of Facilities, Information and Asset Management; Human Resource Management; and Office of Inspector General;

37.5.33.5 The Chair of this group may extend membership to representatives from Component CIOs, at his/her discretion.

37.5.33.6 The Chair of this group may invite additional participants from DOT and other organization at his/her discretion to address complex cybersecurity topics, emerging threats or to obtain insight into best practices.

(Table of Contents)

Section 37.6 Dates

37.6.1 This Departmental Cybersecurity Policy is effective as of the date signed.

(Table of Contents)

Section 37.7 Cancellations

37.7.1 This Departmental Cybersecurity Policy cancels the following DOT Information Assurance Policies and Guidance:

a) DOT Order 1351.2 ACCESS CONTROLS (AC)
b) DOT Order 1351.3 CONFIGURATION MANAGEMENT (CM)
c) DOT Order 1351.4 SYSTEM AND INFORMATION INTEGRITY (SI)
d) DOT Order 1351.5 SECURITY AWARENESS AND TRAINING (AT)
e) DOT Order 1351.6 CERTIFICATION, ACCREDITATION AND SECURITY
f) ASSESSMENTS (CA)
g) DOT Order 1351.7 SYSTEM AND COMMUNICATIONS (SC)
h) DOT Order 1351.8 AUDIT AND ACCOUNTABILITY (AU)
i) DOT Order 1351.9 RISK ASSESSMENT (RA)
j) DOT Order 1351.10 SECURITY PLANNING (PL)
k) DOT Order 1351.11 CONTINGENCY PLANNING (CP)
l) DOT Order 1351.12 SYSTEM ACQUISITION (SA)
m) DOT Order 1351.13 MAINTENANCE (MA)
n) DOT Order 1351.14 MEDIA PROTECTION (MP)
o) DOT Order 1351.15 IDENTIFICATION AND AUTHENTICATION (IA)
p) DOT Order 1351.16 PHYSICAL AND ENVIRONMENTAL (PE) CONTROLS
q) DOT Order 1351.17 INCIDENT RESPONSE (IR)
r) DOT Order 1351.18 PERSONNEL SECURITY (PS)
s) DOT Order 1351.30 INFORMATION ASSURANCE PLANS OF ACTION AND MILESTONES

(Table of Contents)

Section 37.8 Compliance

37.8.1 The DOT Components must comply with and support the implementation of a Departmental Cybersecurity Program, to include compliance with Federal requirements and programmatic policies, standards, procedures, and information system security controls. This policy applies to all DOT Components (and organizations conducting business for and on behalf of the Department through contractual relationships when using DOT IT resources). This policy does not supersede any other applicable law, higher-level agency directive, or existing labor management agreement in place as of the effective date of this policy.

37.8.2 Departmental officials must apply this Departmental Cybersecurity Policy to employees, contractor personnel, interns and other non-government employees. All DOT Components collecting or maintaining information, or using or operating information systems on behalf of the Department, are also subject to this Departmental Cybersecurity Policy. The content of this Departmental Cybersecurity Policy must be incorporated into applicable contract language, as appropriate.

37.8.3 Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act, Trade Secrets Act).

DOT Components must comply with this Policy in accordance with statements outlined in Section 3 of this policy, *Scope and Applicability*.

37.8.4 Non-compliance with the Departmental Cybersecurity Policy and its associated Departmental Cybersecurity Compendium, including failure to resolve or report high risk vulnerabilities in a timely manner, must be reported to the appropriate DOT Component for referral to DOT senior management for resolution.

37.8.5 Depending on the severity of non-compliance, and at the discretion of management, consequences will apply until satisfactory corrective actions have been taken. Consequences may include, but are not limited to, any, or a combination of the following:

37.8.5.1 Reprimand.

37.8.5.2 Suspension of current and/or future funding.

37.8.5.3 Information system disconnection.

(Table of Contents)

Section 37.9 Waivers

37.9.1 Compliance with this policy is mandatory.

37.9.2 DOT Component Heads can request that the DOT CIO grant a waiver of compliance based on a compelling business reason. The request must include: (1) justification, (2) what measures or compensating controls already exist, (3) risk acceptance, (4) risk mitigation measures, (5) waiver period, and (6) milestones to achieve compliance.

37.9.3 If a material weakness is reported in an audit report, and the control weakness is not scheduled to be remediated within twelve (12) months, the DOT Component Head must submit a waiver request to the DOT CIO. If the material weakness is against a financial management system, the DOT CFO must also approve the waiver request before sending to the DOT CIO.

37.9.4 All waiver requests must identify the POA&M for bringing the information system procedures or control weakness into compliance. In all cases, waivers must be requested for an appropriate period based on a reasonable remediation strategy.

37.9.5 DOT Component Heads may request an exception whenever they are unable to bring an information system control weakness into compliance or when it requires a permanent exception to DOT policy. Exceptions are generally limited to information systems that are unable to comply due to detrimental impact to mission, excessive costs, and/or clearly documented end of platform life for non-essential information systems within eighteen (18) months, commercial-off-the-shelf (COTS) products that cannot be configured to support the control requirement, etc. This request is made, by the respective ISSM through the DOT Component Head to the DOT CIO and must include the operational justification, risk acceptance, and risk mitigation measures.

The resulting risk must be approved and accepted by the AO and by the DOT CFO if the information system is a financial or mixed financial system.

(Table of Contents)

Section 37.10 Audit Procedures

37.10.1 In order to ensure that the Department provides appropriate accountability for information security, and that the DOT OCIO provides active support and oversight of monitoring and improvement of the Departmental Cybersecurity Program, the DOT CISO must:

37.10.1.1 Develop and implement an oversight and compliance function to provide the required guidance and reviews to meet FISMA and other government-wide cybersecurity requirements;

37.10.1.2 Conduct annual compliance reviews of DOT Component Cybersecurity Programs;

37.10.1.3 Develop and manage POA&Ms for the Departmental Cybersecurity Program reporting progress to the DOT CIO and Secretary of Transportation; and

37.10.1.4 Monitor DOT Component efforts to address weaknesses in their respective Cybersecurity Programs and information systems.

37.10.2 Because of the dynamic nature of cybersecurity, DOT information systems, and information technology and associated services, the DOT CISO must:

37.10.2.1 Facilitate the review of the Departmental Cybersecurity Policy and the Departmental Cybersecurity Compendium on an annual basis. The DOT CISO will identify and involve appropriate DOT Component senior management, security professionals, and other stakeholders in the annual review to comment on proposed updates to the policy to address evolving threats, changes to existing government-wide cybersecurity regulations, policy and guidance, and emerging technology and information technology service delivery models, and to implement adjustments to the policy deemed necessary to improve its effectiveness based on feedback from DOT Component personnel;

37.10.2.2 Issue updates to this policy based on the results of these reviews in accordance with DOT CIO Directives policy. These updates may consist of change pages to existing policy, procedures, and guidance as well as new Departmental Cybersecurity Compendium policy, procedures, and guidance;

37.10.2.3 Perform an ongoing function to identify new cybersecurity requirements for the Department and new cybersecurity threats to DOT information systems. The DOT CISO must determine if DOT can address the new requirement or threat through the ongoing annual review and update process described above; and

37.10.2.4 If due to the nature of the requirement or threat, the DOT CISO deems more urgent action it required, the DOT CISO will initiate appropriate actions and coordination to support development and review of policy, guidance, or other required action. The DOT CIO will communicate direction to effected DOT organizations. The DOT CISO will ensure the requirement and the resulting guidance issued by the DOT CIO is incorporated into the ongoing review and update process to be formally incorporated into the Departmental Cybersecurity Policy and Departmental Cybersecurity Compendium accordingly.

(Table of Contents)

Section 37.11 Approval

This policy has been approved and issued under the authority granted to the Secretary of Transportation, Chief Information Officer in accordance with Public Law 104-106, Clinger-Cohen Act of 1996, and the Federal Information Security Management Act (FISMA) of 2002.

7/7/2011

Mr. Nitin Pradhan
DOT Chief Information Officer

Date

(Table of Contents)

Appendix A Authorities and Guidance

Legislation

a) E-Government Act [includes FISMA] (P.L. 107-347), December 2002.
b) Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.
c) Paperwork Reduction Act (P.L. 104-13), May 1995.
d) USA PATRIOT Act (P.L. 107-56), October 2001.
e) Privacy Act of 1974 (P.L. 93-579), December 1974, 5 USC 552a.
f) Freedom of Information Act (FOIA), 5 U.S.C. § 552.
g) Health Insurance Portability and Accountability Act (P.L. 104-191), August 1996.

National Policy, Directives and Memorandum

a) Code of Federal Regulations, Title 5, Administrative Personnel, Section 731.106, Designation of Public Trust Positions and Investigative Requirements (5 C.F.R. 731.106).

b) Code of Federal Regulations, Title 5 Administrative Personnel, Subpart C—Employees Responsible for the Management or Use of Federal Computer Systems, Section 930.301 through 930.305 (5 C.F.R 930.301-305).

c) Executive Order, Controlled Unclassified Information, 4 November 2010.

d) Federal Continuity Directive 1 (FCD 1), Federal Executive Branch National Continuity Program and Requirements, February 2008.

e) Homeland Security Presidential Directive 7, Critical Infrastructure Identification, Prioritization, and Protection, December 2003.

f) Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 2004.

g) Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, Management of Federal Information Resources, November 2000.

h) Office of Management and Budget, Federal Enterprise Architecture Program Management Office, FEA Consolidated Reference Model Document, Version 2.3, October 2007.

i) Office of Management and Budget, Federal Segment Architecture Methodology (FSAM), January 2009.

j) Office of Management and Budget Memorandum M-01-05, Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy, December 2000.

k) Office of Management and Budget Memorandum M-02-01, Guidance for Preparing and Submitting Security Plans of Action and Milestones, October 2001.

l) Office of Management and Budget Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting, August 2003.

m) Office of Management and Budget Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 2003.

n) Office of Management and Budget Memorandum M-04-04, E-Authentication Guidance for Federal Agencies, December 2003.

o) Office of Management and Budget Memorandum M-04-26, Personal Use Policies and File Sharing Technology, September 2004.

p) Office of Management and Budget Memorandum M-05-08, Designation of Senior Agency Officials for Privacy, February 2005.

q) Office of Management and Budget Memorandum M-05-24, Implementation of Homeland Security Presidential Directive 12—Policy for a Common Identification Standard for Federal Employees and Contractors, August 2005.

r) Office of Management and Budget Memorandum M-06-15, Safeguarding Personally Identifiable Information, May 2006.

s) Office of Management and Budget Memorandum M-06-16, Protection of Sensitive Information, June 2006.

t) Office of Management and Budget Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, July 2006.

u) Office of Management and Budget Memorandum, Recommendations for Identity Theft Related Data Breach Notification Guidance, September 2006.

v) Office of Management and Budget Memorandum M-07-11, Implementation of Commonly Accepted Security Configurations for Windows Operating Systems, March 2007.

w) Office of Management and Budget Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 2007.

x) Office of Management and Budget Memorandum M-07-18, Ensuring New Acquisitions Include Common Security Configurations, June 2007.

y) Office of Management and Budget Memorandum M-08-09, New FISMA Privacy Reporting Requirements for FY 2008, January 2008.

z) Office of Management and Budget Memorandum M-08-21, FY08 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, July 2008.

aa) Office of Management and Budget Memorandum M-08-22, Guidance on the Federal Desktop Core Configuration (FDCC), August 2008.

bb) Office of Management and Budget Memorandum M-08-23, Securing the Federal Government’s Domain Name System Infrastructure, August 2008.

cc) Update on the Trusted Internet Connections Initiative, M-09-32, September 17, 2009.

dd) FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, M-09-29, August 20, 2009.

ee) Information Technology Management Structure and Governance Framework, M-09-02, October 21, 2008.

ff) FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, M-10-15, April 21, 2010.

gg) Office of Management and Budget Memorandum M-11-11, Continued Implementation of Homeland Security Presidential Directive (HSPD) 12–Policy for a Common Identification Standard for Federal Employees and Contractors, February 3, 2011.

National Standards

a) National Institute of Standards and Technology Federal Information Processing Standards Publication 140-2, Security Requirements for Cryptographic Modules, May 2001.

b) National Institute of Standards and Technology Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004.

c) National Institute of Standards and Technology Federal Information Processing Standards Publication 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006.

d) National Institute of Standards and Technology Federal Information Processing Standards Publication 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006.

Departmental Cybersecurity Policy

a) Departmental Cybersecurity Compendium (current version).

National Guidelines

a) The National Institute of Standards and Technology (NIST) publish and maintain guidelines for information and cybersecurity. These guidelines, published as a series of "special publications", are provided as guidelines to Federal agencies to assist in implementation of their Cybersecurity Programs. These guidelines are used as the basis for Departmental Cybersecurity Compendium supplemental policy, procedures and standards. The special publications are located at: http://csrc.nist.gov/publications/PubsSPs.html

Appendix B Glossary

Access — Ability to make use of any information system resource. (Defined in NIST SP 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*)

Authorization — The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. (Defined in NIST SP 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems*)

Authorizing Official — A senior (Federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. (Defined in NIST SP 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*)

Authorizing Official Designated Representative — An organizational official acting on behalf of an authorizing official in carrying out and coordinating the required activities associated with security authorization. (Defined in NIST SP 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*)

Availability — Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system. (Defined in FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*)

Breach — The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic. (Defined in OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*)

Compensating Controls — Management, operational, or technical controls employed by an organization, in lieu of prescribed controls in the Low, Moderate, or High security National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 control baselines, which provide equivalent or comparable protection for an information system. (Defined in FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*)

Confidentiality — Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (Defined in FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*)

Configuration Management (CM) — A discipline applying technical and administrative direction and surveillance to: identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements. (Defined in IEEE 610.12, *Standard Glossary of Software Engineering Terminology*)

Contingency Plan (CP) — Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster. (Defined in NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Information Technology Systems*)

Continuous Monitoring -- A continuous monitoring program requires the active involvement of information system owners and common control providers, chief information officers, senior information security officers, and authorizing officials. The monitoring program allows an organization to: (i) track the security state of an information system on a continuous basis; and (ii) maintain the security authorization for the system over time in highly dynamic environments of operation with changing threats, vulnerabilities, technologies, and missions/business processes. Documenting information system changes as part of routine SDLC processes and assessing the potential impact those changes may have on the security state of the system is an essential aspect of continuous monitoring, maintaining the current authorization, and supporting a decision for reauthorization when appropriate. Formal reauthorization actions are avoided in situations where the continuous monitoring process provides authorizing officials the necessary information to manage the potential risk arising from changes to the information system or its environment of operation. Organizations maximize the use of status reports and security state information produced during the continuous monitoring process to minimize the level of effort required if a formal reauthorization action is required. Formal reauthorization actions occur at the discretion of the authorizing official in accordance with federal or organizational policy. (Defined in NIST SP 800-37)

Cybersecurity- The performance of information security, network security, and information assurance to protect information systems and information infrastructure along with the sensitive data they contain from unauthorized access, use, disclosure, disruption, modification, or destruction from threats that can impact confidentiality, integrity, and availability of the information, information technology services, and communications.

Cybersecurity Program – A program created at the Departmental and Component levels to implement mandatory government-wide information security and cybersecurity regulations, policies, standards and guidance. The program includes planning, implementation, and monitoring to ensure compliance with requirements and adoption of effective processes and best practices to provide protection of Departmental and Component information systems and the business process and mission delivery these information support.

Enterprise Architecture (EA) — A strategic information asset base, which defines the business, the information necessary to operate the business, the technologies necessary to support the business operations, and the transitional processes necessary for implementing new technologies in response to the changing business needs. It is a representation or blueprint. (Defined in the Chief Information Officers Council *Federal Enterprise Architecture Framework Version 1.1* as "Federal enterprise architecture")

Federal Information Security Management Act (FISMA) -- The E-Government Act (P.L. 107-347) recognizes the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), emphasizes the need for organizations to develop, document, and implement an organization-wide program to provide security for the information systems that support its operations and assets. (NIST SP 800-39, *Managing Information Security Risk*)

Integrated Program Planning and Management (IPPM) – A framework, set of processes and activities necessary to ensure that investments in IT programs and projects are properly planned and managed throughout their lifecycle. It leverages principles and best practices in the areas of Enterprise Architecture, Capital Planning and Investment Control, Records Management, and Security Management to provide an integrated roadmap for all DOT IT investments.

Identification — The process of discovering the true identity (i.e., origin, initial history) of a person or item from the entire collection of similar persons or items. (Defined in FIPS 201-1, *Personal Identity Verification for Federal Employees and Contractors*)

Incident — A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. (Defined in NIST SP 800-61 Rev.1, *Computer Security Incident Handling Guide*)

Incident Response Plan — The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of malicious cyber attacks against an organization's information systems(s). (Defined in NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Information Technology Systems*)

Independent Assessor — Any individual or group capable of conducting an impartial assessment of security controls employed within or inherited by an information system. (Defined in NIST SP 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*)

Information — Any communication or representation of knowledge such as facts, data, or opinions in any medium or form to include textual, numerical, graphic, cartographic, narrative, or audiovisual forms. (Defined in OMB Circular A-130, *Transmittal Memorandum #4, Management of Federal Information Resources*, 6(a))

Information Technology -- Any equipment or interconnected system or subsystem of equipment that is 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 an agency whether the agency 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 that is acquired by a Federal contractor incidental to a Federal contract. (Defined in Clinger-Cohen Act of 1996, sections 5002, 5141 and 5142)

Information Resources — Information and related resources, such as personnel, equipment, funds, and IT. (Defined in 44 U.S.C., SEC. 3502)

Information Security Measures — Activities used to facilitate decision making and improve performance and accountability through the collection, analysis, and reporting of relevant performance-related data. (Defined in NIST SP 800-55 Rev. 1, *Performance Measurement Guide for Information Security*)

Information Security Program Plan — Formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements. See also “Security Plan.” (Defined in NIST SP 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach)*

Information System — A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (Defined in NIST SP 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems*)

Information System Contingency Plan (ISCP) — Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disasters.. (Defined in NIST SP 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems*)

Information Technology Security Architecture — A description of security principles and an overall approach for complying with the principles that drive the system design (i.e., guidelines on the placement and implementation of specific security services within various distributed computing environments). (Defined in NIST SP 800-27A, *Engineering Principles for Information Technology Security [A Baseline for Achieving Security]*)

Integrity — Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. (Defined in FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*)

Interconnection Security Agreement (ISA) — An agreement established between the organizations that own and operate connected information systems to document the technical requirements of the interconnection. The ISA also supports a Memorandum of Understanding or Agreement (MOU/A) between the organizations. (Defined in NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*)

Memorandum of Understanding/Agreement (MOU/A) — A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. In this guide, an MOU/A defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection. (Defined in NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*)

Mobile Devices — Portable cartridge/disk-based removable storage media (e.g., floppy disks, compact disks, USB flash drives, and other flash memory cards/drives that contain non-volatile memory). Portable computing and communication devices with information storage capability (e.g., notebook, laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). (Defined in NIST SP 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems*)

Patch — An additional piece of code developed to address a problem in an existing piece of software. (Defined in NIST SP 800-40 Version 2.0, *Creating a Patch and Vulnerability Management Program*)

Personal Identification Verification (PIV) Card — A secure and reliable form of identification credential issued by the Federal Government to its employees and contractors. This credential is intended to authenticate an individual who requires access to federally controlled facilities, information systems, and applications. (Defined in FIPS 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*)

Personally Identifiable Information (PII) — Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. (Defined in OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*) Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history and information which can be used to distinguish or trace an individual's identify, such as their name, SSN, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual. (Defined in OMB M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency IT Investments*)

Plans of Action & Milestones (POA&M) — A document that identifies tasks needing to be accomplished, and details on the resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. (Defined in OMB M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*)

Cybersecurity Policy — The rules and regulations set by an organization that define the purpose of the program and its scope within an organization; assigns responsibilities for direct program implementation, as well as other responsibilities to related offices (e.g., Chief Information Office); and addresses compliance issues. A program policy sets organizational and strategic direction for security and assigns resources for the program's implementation. (Defined in NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*)

Portable Storage Media — Any device that can store data electronically and is portable, such as portable hard drives, universal serial bus (USB) drives, secure digital (SD) card media, compact discs – read only memory (CD-ROMs), and digital video discs (DVDs). (Defined in DOT Standard 2008-0007.001S, *DOT Standard for Encryption*)

Privacy — The appropriate use of personal information. (Defined in the International Association of Privacy Professionals site glossary)

Privacy Incident — An incident that involves personally identifiable information or protected health information. (Defined in US-CERT Quarterly Trends and Analysis Report, Volume 1, Issue 2, adapted)

Privileged Accounts — A user account for a person that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. (Defined in CNSSI 4009, National Information Assurance Glossary, adapted)

Risk — A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs, and (ii) the likelihood of occurrence. Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. (Defined in NIST SP 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems*)

Risk-Based Decisions -- Decisions based on trade-offs between fulfilling and improving organizational missions and business functions and managing the many types and sources of risk that must be considered in their risk management responsibilities. (Defined in NIST SP 800-39 *Managing Information Security Risk*)

Risk Assessment — The process of identifying risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place. This term is synonymous with risk analysis. (Defined in NIST SP 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems*)

Risk Executive (Function) — An individual or group within an organization that helps to ensure that: (i) security risk-related considerations for individual information systems, to include the authorization decisions, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its missions and business functions and (ii) managing information system-related security risks is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success. (Defined in NIST SP 800-37 Rev. 1 or later, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach)*

Risk Management Framework (RMF) — The new six-step process established in NIST SP 800-37 Rev.1, which is the transformation of the previous Certification and Accreditation (C&A) process. The RMF changes the traditional focus of C&A as a static, procedural activity to a more dynamic approach that provides the capability to more effectively manage information system-related security risks in highly diverse environments of complex and sophisticated cyber threats, ever-increasing system vulnerabilities, and rapidly changing missions. (Defined in NIST SP 800-37 Rev. 1 or later, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach)*

Role-Based Training — Training focused on the knowledge, skills, and abilities an individual needs to perform the IT security responsibilities specific to each of his or her roles in the organization. (Defined in NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*)

Routine Use — The use of such record for a purpose which is compatible with the purpose for which it was collected. (Defined in the Privacy Act of 1974)

Security Assessment Report — Prepared by the security control assessor,[8] this report provides the results of the assessment of the implementation of security controls identified in the security plan to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the specified security requirements. The SAR can also contain a list of recommended corrective actions or deficiencies identified in the security controls. (Defined in NIST SP 800-37 current version, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*)

Security Authorization — See "Authorization." (Defined in NIST SP 800-37 (current version)

Security Control Assessor — An individual, group, or organization responsible for conducting a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an information system to determine the overall effectiveness of the controls (i.e., the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system). (Defined in NIST SP 800-37, current version, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*)

Security Controls — The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system which, taken together, adequately protect the confidentiality, integrity, and availability of the system and its information. (Defined in FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*)

Sensitive Information -- Information in which the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. (Defined in Glossary of Key Information Security Terms, NIST IR 7298 Revision 1, February 2011)

Servicing Security Organization (SSO) -- The organizational element that is responsible for providing security services to a particular DOT administration or organization.

System Development Life Cycle (SDLC) — The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation

[8] Security control assessor is a new term (role) in NIST SP 800-37 Rev.1. Security control assessors may be called certification agents in some organizations.

and maintenance, and ultimately its disposal that instigates another system initiation. (Defined in NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Information Technology Systems*)

System of Records (SOR) — A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. (Defined in the Privacy Act of 1974)

System Security Plan (SSP) — An analysis of how information is handled: 1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; 2) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and 3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. See also "Security Plan." (Defined in FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*)

User — Individual or (system) process acting on behalf of an individual, who is authorized to access an information system. (Defined in CNSSI 4009, National Information Assurance Glossary, adapted)

Vulnerability — A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. (Defined in NIST SP 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems*)

Appendix C Acronyms

AO	Authorizing Official
BRT	Breach Response Team
CA	Certification Agent
CFO	Chief Financial Officer
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CISO	Chief Information Security Officer
CM	Configuration Management
CO	Contracting Officer
COOP	Continuity of Operations Plan
COTR	Contracting Officer's Technical Representative
CP	Contingency Plan
CPIC	Capital Planning and Investment Control
CSAM	Cyber Security Assessment and Management
CSIRC	Computer Security Incident Response Center
CSIRT	Computer Security Incident Response Team
DOT	Department of Transportation
FAR	Federal Acquisition Regulation
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act of 2002
FOIA	Freedom of Information Act
HSPD	Homeland Security Presidential Directive
IA	Information Assurance

ISCP	Information System Contingency Plan
ISSO	Information Systems Security Officer
IT	Information Technology
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
OA	Operating Administration
OCIO	Office of the Chief Information Officer
OHRM	Office of Human Resources Management
OIG	Office of Inspector General
OMB	Office of Management and Budget
OSPE	Office of the Senior Procurement Official
PII	Personally Identifiable Information
POA&M	Plans of Action and Milestones
POC	Point of Contact
RA	Risk Assessment
RoB	Rules of Behavior
RMF	Risk Management Framework
SAOP	Senior Agency Official for Privacy
SAR	Security Assessment Report
SCA	Security Control Assessor
SOR	System of Records
SP	Special Publication
SSP	System Security Plan
US-CERT	United States Computer Emergency Readiness Team