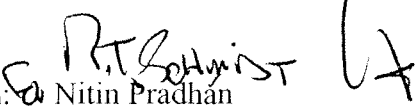


# Memorandum

**U.S. Department of Transportation**  
Office of the Secretary  
of Transportation

---

Subject: Dissemination of OST Cybersecurity Policy (Order 1351.37(D))

From:  Nitin Pradhan  
Chief Information Officer  
Office of the Chief Information Officer

Date: 02/03/12

Reply to: T. Smith, OST CIO

To: Office of the Secretary, Secretarial Office Heads

## SUMMARY

The OST Cybersecurity Policy (DOT Order 1351.37[D]) specifies high-level cybersecurity policy for the Office of the Secretary. The Order is an appendix to DOT Order 1351.37 Departmental Cybersecurity Policy and defines roles at the Department, OST and information system levels. It also includes associated cybersecurity responsibilities necessary to implement the DOT Cybersecurity Program and comply with mandatory security requirements for OST systems.

The policy may be accessed online at:

<https://one.dot.gov/ost/s80/S81/S81new/CIOP/Forms/CIOP.aspx>.

## BACKGROUND

The DOT Order 1351.37, Departmental Cybersecurity Policy, and its supplement, the Departmental Cybersecurity Compendium, were issued to implement mandatory requirements specified for all Federal agencies in the Federal Information Security Management Act (FISMA) and guidance issued by the Office of Management and Budget (OMB), National Institutes of Standards and Technology (NIST) and the Department of Homeland Security (DHS). Given the unique operating and management environment of the OST offices, it was determined that the Departmental Cybersecurity Policy and Compendium, while applicable to OST and its Offices, was not implementable as written. As such, OCIO made specific modifications to address OST's requirements. All policies, procedures, standards and guidance required of DOT Components under the Departmental Cybersecurity Policy and its companion Departmental Cybersecurity Compendium apply to OST, except those set forth in Sections

37.5.16 through 37.5.17 of the Departmental Cybersecurity Policy and as otherwise specified in this policy. Issuing DOT Order 1351.37(D) enables DOT to address current regulations, policies and standards required of DOT, as well as address a number of OIG recommendations involving weaknesses and gaps in securing the DOT environment.

The development and subsequent negotiation of the OST provisions were led by S-81 with support from S-80 using a collaborative approach that involved information system security professionals and business owners from all OST offices. The resulting DOT Order 1351.37(D) completed one formal round of review while the Departmental Cybersecurity Policy (Order 1351.37) completed three rounds of formal review in accordance with CIO Policy Directive 1351.1 “IT Directives Management”.

The resulting DOT Order 1351.37(D) completed one formal round of review while the Departmental Cybersecurity Policy (Order 1351.37) completed three rounds of formal review in accordance with CIO Policy Directive 1351.1 “IT Directives Management”. Responsibility for this policy is assigned to Tracey Smith, Acting Chief Information Officer, OST.

#### **ACTION REQUIRED**

All Departmental Secretarial Offices must ensure the new DOT Order is appropriately disseminated to those in its organization who perform the responsibilities listed in DOT Order 1351.37 (D).

Should you have any questions, please contact Ms. Tracey Smith on (202) 385-2721 or [tracey.smith@dot.gov](mailto:tracey.smith@dot.gov).

## **Appendix D: Office of the Secretary Cybersecurity Policy Supplement**

### **TABLE OF CONTENTS**

<b>D.1</b>	Purpose.....	2
<b>D.2</b>	Background .....	2
<b>D.3</b>	Scope and Applicability .....	4
<b>D.4</b>	Policy.....	5
<b>D.5</b>	Roles and Responsibilities .....	7
<b>D.6</b>	Dates.....	10
<b>D.7</b>	Cancellations .....	10
<b>D.8</b>	Compliance.....	10
<b>D.9</b>	Waivers.....	11
<b>D.10</b>	Audit Procedures .....	11
<b>D.11</b>	Approval .....	11
<b>D.12</b>	Attachment 1 Authorities and Guidance .....	12
<b>D.13</b>	Attachment 2 Glossary .....	13
<b>D.14</b>	Attachment 3 Acronyms .....	14

## **D.1 Purpose**

The Departmental Cybersecurity Policy (DOT Order 1351.37) 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 Office of the Secretary (OST) oversees the formulation of national transportation policy and promotes intermodal transportation. Other responsibilities range from negotiation and implementation of international transportation agreements, assuring the fitness of US airlines, enforcing airline consumer protection regulations, issuance of regulations to prevent alcohol and illegal drug misuse in transportation systems and preparing transportation legislation. The organizations that comprise OST are referred to as Secretarial Offices. OST is organized differently and has a mission different from that of DOT Operating Administrations (OA). As such, the DOT Office of the Chief Information Officer (OCIO) determined that it is necessary to specify cybersecurity policy to address these unique organizational needs.

The purpose of this appendix is to establish the cybersecurity policies, processes, procedures and standards for OST to meet its unique needs in alignment with the overall Departmental Cybersecurity Policy. This policy is a supplement to the Departmental Cybersecurity Policy and its companion Departmental Cybersecurity Compendium. This policy does not supersede DOT Order 1351.37 or any other applicable law, such as the Federal Information Security Management Act (FISMA), or higher level Government-wide directive, policy, or guidance such as the Office of Management and Budget (OMB) circulars and memoranda.

(Table of Contents)

## **D.2 Background**

DOT is comprised of OAs, Boards (such as the Surface Transportation Board), and the Office of the Inspector General (OIG). The Departmental Cybersecurity Policy collectively refers to these organizations as “DOT Components” and establishes policy, roles, and responsibilities for these organizations. Through development of the Departmental Cybersecurity Policy, the OCIO determined that significant differences in the organization of OST necessitated the need to devise a supplemental policy for OST.

The DOT OCIO, under the responsibility and authority granted by the Secretary of Transportation in accordance with Public Law 104-106, Clinger-Cohen Act of 1996, the Federal Information Security Management Act of 2002 and OMB Memo M-09-02, Information Technology Management Structure and Governance Framework, issues this policy to ensure that an OST Cybersecurity Program is developed, documented, and implemented to provide security for all Secretarial Offices information systems, information technology, networks, and data that support departmental operations.

The FISMA requires Federal agencies to adopt security guidance and standards issued by the OMB and the National Institutes of Standards and Technology (NIST). The foundational standard known as the NIST Risk Management Framework (RMF) specifies that:

- Secretarial Office Heads and other 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 mission and business functions across OST.
- Effectively managing information security risk in OST requires assignment of risk management responsibilities to senior leaders/executives.
- There must be ongoing recognition and understanding by Secretarial Office Heads and other senior officials of the information security risks to OST operations and assets, individuals, other organizations, and the Nation arising from the operation and use of information systems.
- OST 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.
- Secretarial Office Heads and other senior officials 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.

In 2010, the OCIO issued “IT Governance Guidance”<sup>1</sup>. This memo outlines the roles and responsibilities of “business system owners”, “service providers”, “customers” and the applicable governance bodies and processes. The Secretarial Offices fulfill the “business system owner” role while the OCIO performs the role of “service provider”.

All government agencies seek to create efficiency in the services they provide. The Office of Management and Budget (OMB) and Congress requires agencies to consolidate functions and services to reduce cost. In considering the unique needs of the Secretarial Offices, current IT governance of Secretarial Offices information systems, and the need to increase security and achieve compliance with Clinger-Cohen Act and FISMA, the OCIO seeks to enhance and augment IT governance of Secretarial Offices to achieve efficiency, IT governance and Cybersecurity compliance.

---

<sup>1</sup> IT Governance Guidance, Nitin Pradhan, DOT CIO, 11 June 2010.

(Table of Contents)

## **D.3 Scope and Applicability**

D.3.1 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.

D.3.2 This OST Cybersecurity Policy is issued under the DOT OCIO'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.

D.3.3 All Secretarial Offices must comply with the OST Cybersecurity Policy, the Departmental Cybersecurity Compendium, and, as indicated herein, the Departmental Cybersecurity Policy.<sup>2</sup>

D.3.4 The OST Cybersecurity Policy applies to:

D.3.4.1 All Secretarial Offices conducting DOT business, operating DOT information systems, and collecting and/or maintaining information for, or on behalf of DOT;

D.3.4.2 All OST permanent and temporary employees, consultants, contractors, interns, authorized personnel and other non-government employees using DOT information systems and information technology resources; and

D.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.

D.3.5 Conversely, this OST Cybersecurity Policy does NOT apply to the following:

D.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.

---

<sup>2</sup> The Compendium contains policy which has the full force of the DOT CIOP Order 1351.37. The Compendium is a collection of supplemental cybersecurity policies as well as standards, procedures and other guidance necessary to ensure the Department meets government-wide cybersecurity requirements and to establish Department-wide standardized processes.

D.3.5.2 Any public users of any DOT information systems implemented for the express purpose of public access and dissemination of information.

(Table of Contents)

## **D.4 Policy**

### ***OCIO Framework***

D.4.1 The OCIO must provide OST Secretarial Offices business systems management support services enabling the OCIO to take responsibility for and execute requirements for IT Security for all non-major Secretarial Offices' information systems (OST Systems Portfolio). The OST Systems Portfolio shall consist of all non-major information systems for which the Secretarial Offices are the primary functional business requirements owner(s). Non-major information systems are defined as "business systems" not meeting the requirement of "major" system or otherwise agreed to by the OCIO and the OST Office owning the functional business requirements of the system. "Major" OST information systems are those OST systems which have an OMB Exhibit 300 approved by the DOT OCIO and OMB.

D.4.1.1 The OCIO must provide an appropriate, fully allocated resource to serve as the Information Systems Security Manager (as defined by DOT Cybersecurity Policy) for the OST Systems Portfolio. The OST ISSM shall report to the OST CIO, and cybersecurity and information assurance shall compromise the entirety of the position duties.

D.4.2 The OCIO must provide Security governance and support for the OST Systems Portfolio. Security governance is defined as oversight and guidance to ensure IT systems are secured in accordance with DOT policy, and commensurate with the level of risk.

D.4.2.1 The IT security support provided for the OST Systems Portfolio consists of the following roles and associated responsibilities as defined by the NIST's Risk Management Framework: Authorizing Official Designated Representative (AODR), System Owner, Information System Security Officer (ISSO), Security Control Assessor (SCA), and Technical Support Staff.<sup>3</sup>

### ***Secretarial Office Responsibilities***

D.4.3 The Secretarial Offices must for the OST Systems Portfolio execute the responsibilities of "business owners" and "customers" as defined by the IT Governance Guidance.<sup>4</sup> *Business owner* is defined as the, "spokesperson for the IT service initiative and the owner of the business, function, and funding requirements for the system/service throughout the business's life cycle, from concept to disposal. A *customer* is the focus and the recipient of a business service. The business system is implemented to address the business needs of the

---

<sup>3</sup> Refer to DOT Order 1351.37, Departmental Cybersecurity Policy for a definition of these roles.

<sup>4</sup> Refer to "IT Governance Guidance", Nitin Pradhan, DOT CIO, 11 June 2010 for definition of these roles.

customer. The success of the business system is determined by the value it provides to its customers.

D.4.4 Secretarial Offices must, at a minimum, perform the role of Information Owner as outlined in the Departmental Cybersecurity Policy for all systems assigned to the OST Systems Portfolio.

D.4.4.1 Secretarial Offices must retain validation and certification of functional system requirements and workflow behavior (as appropriate).

D.4.4.2 Secretarial Offices must retain the requirement to identify business system and functional risks and support the development and implementation of business risk mitigation plans.

D.4.5 Secretarial Offices that are the business owner of OST “Major” information systems may retain or be assigned additional IT and Cybersecurity roles. The OCIO and the Secretarial Office business owner must document and jointly approve of the role assignment between the parties for OST Major information systems. If OST is assigned the role of “service provider” or is required to perform any other Cybersecurity roles aside from the ISSM for OST Portfolio Systems to support the OST Major information system, a Service Level Agreement (SLA) must accompany the role assignment and specify resources to be provided to OCIO to support the roles, responsibilities and associated services assigned.

D.4.6 Together the OCIO, and Secretarial Offices must ensure OST implements and complies with the policies specified herein and the Departmental Cybersecurity Policy and its companion Compendium 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.

D.4.7 All policies, procedures, standards and guidance required of DOT Components under the Departmental Cybersecurity Policy and its companion Departmental Cybersecurity Compendium apply to OST, except those set forth in Sections 37.5.16 through 37.5.17 of the Departmental Cybersecurity Policy and as otherwise specified in this policy. Specific changes include:

D.4.7.1 The Program-level roles specified in the Departmental Cybersecurity Policy are required functions for Secretarial Offices and the OST CIO unless otherwise agreed and documented. The need for these roles will be determined by the OST CIO and the appropriate Secretarial Offices upon implementation of this policy and assigned or identified accordingly.

D.4.8 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.

(Table of Contents)

## **D.5 Roles and Responsibilities**

This section defines the roles key to implementing the OST Cybersecurity Program across the Secretarial Offices along with cybersecurity-specific responsibilities associated with each role and is an appendix to the Roles and Responsibilities listed in the Departmental Cybersecurity Policy in section 5 Order 1351.37 describes roles and responsibilities at the Component Level. Where the Component-level role in Order 1351.37 and the OST-level role in Appendix D are the same, responsibilities that are applicable in OST are incorporated by reference. Any roles and/or responsibilities that were not addressed in Order 1351.37 are defined in this section.

### **Department Level**

- DOT Chief Information Officer (CIO)
- DOT Chief Information Security Officer (CISO)

### **OST Level**

- Secretarial Office Heads
- OST CIO
- OST ISSM

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

D.5.1 The cybersecurity-related responsibilities of the **DOT Chief Information Officer** are listed in DOT Order 1351.37.5.2. Additional responsibilities pertaining to OST include:

D.5.1.1 Designating the OST CIO with overall accountability for ensuring OST appropriately implements information security protections in addition to other non-information security duties;

D.5.1.2 Delegating to the OST CIO the authority to ensure compliance of OST with the OST Cybersecurity Program;

D.5.1.3 Appointing the OST ISSM to support the OST CIO in developing and maintaining the OST Cybersecurity Program; and

D.5.1.4 Coordinating with the Secretarial Office Heads to ensure the provision of necessary resources to administer and implement the OST Cybersecurity Program.

D.5.2 The cybersecurity-related responsibilities of the **DOT Chief Information Security Officer** are listed in DOT Order 1351.37.5.3. Additional responsibilities pertaining to OST include:

D.5.2.1 Assisting and advising the OST CIO in the development, documentation, and implementation of the OST 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 OST's operations and assets, including those provided or managed by another Federal organization, a contractor, or other source.

D.5.2.2 Ensuring an OST Cybersecurity Program is developed, documented, and implemented to provide security for all OST Portfolio Systems and OST Major information systems in accordance with the Departmental Cybersecurity Policy;

D.5.2.3 Performing the role of Risk Executive for OST Portfolio Systems unless otherwise delegated to a senior OST 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;

D.5.2.4 Ensuring OST practices its Cybersecurity Program throughout the life cycle of each OST Portfolio System;

D.5.2.5 Ensuring OST Portfolio System assets designated as CRITICAL under Homeland Security Presidential Directive (HSPD)-7 are protected at a Federal Information Processing Standard (FIPS) 199 HIGH level unless a waiver is approved by the DOT CIO; and

D.5.2.6 Establishing appropriate accountability for information security and providing active support and oversight of monitoring and improvement for the information security program for the Secretarial Office;

D.5.2.7 Ensuring an Authorizing Official is appointed for all OST Portfolio Systems, that the appointee is no less than an OST SES-level Government employee and that this appointment is documented and provided to the OST CIO. Unless otherwise specified, the DOT Deputy CIO is the Authorizing Official for the OST Systems Portfolio.

D.5.2.8 Ensuring the protection of OST Portfolio Systems and data for which the OCIO provides IT Security services, by allocating the appropriate resources, including but not limited to 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;

D.5.2.9 Ensuring senior OST officials participate in risk management activities to aid in the determination of the selection and implementation of appropriate IT security using risk-based decisions for operations and IT resources under the control; and

D.5.2.10 Ensuring OST Portfolio Systems investments and programs are reviewed by the OST CIO and accepted by the OST Chief Financial Officer (CFO) to ensure appropriate security requirements are included and resourced as required.

**OST Level: All OST roles must be assigned to and performed by Federal Government employees.<sup>5</sup>**

D.5.3 The cybersecurity-related responsibilities of **Secretarial Office Heads** include:

D.5.3.1 For OST Portfolio Systems for which the OCIO is providing IT Security services, the Secretarial Office business owner of the system must:

D.5.3.1.1 Ensure an Information Owner is appointed for each information systems and that this appointment is documented and provided to the OST CIO;

D.5.3.1.2 Coordinate with the OST CIO, OST CFO, and DOT CIO to plan and budget for the necessary information system protections and support for applicable security requirements through DOT capital planning processes to ensure the necessary resources are included in future budget submissions.

D.5.3.2 For OST information systems not included in the OST Portfolio, the Secretarial Office business owner of the information system must:

D.5.3.2.1 Ensure an Authorizing Official is appointed, that the appointee is no less than an OST SES-level Government employee and that this appointment is documented and provided to the OST CIO;

D.5.3.2.2 In coordination with the DOT CIO, protect OST Major information systems and data by allocating the appropriate resources, including but not limited to 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;

D.5.3.2.3 In coordination with the DOT CIO, ensure senior OST officials provide the appropriate IT security using risk-based decisions for operations and IT resources under their control; and

D.5.3.2.4 In coordination with the DOT CIO, ensure OST Major IT investments or programs are reviewed by the OST CIO to ensure appropriate security requirements are included and necessary resources included in future budget submissions.

D.5.4 The cybersecurity-related responsibilities for the role of **OST CIO** are the same as those of the Component CIO, as listed in DOT Order 1351.37.5.12.1 – 37.5.12.5, 37.5.12.7 – 37.5.12.17. Additional responsibilities include:

D.5.4.1 Working with Secretarial Offices personnel to develop and submit transition plans as required by the DOT CIO for connections that do not pass through a DOT TICAP;

---

<sup>5</sup> Where the DOT Order 1351.37 is incorporated by reference in the roles and responsibilities at the OST level, Component is replaced with OST, Component CIO is replaced with OST CIO, and Component Head is replaced with OST Head for referenced responsibilities.

D.5.4.2 Advising Secretarial Office Heads of Secretarial Offices personnel that do not meet DOT required minimum training requirements;

D.5.4.3 Ensuring a report on the OST Cybersecurity Program and any internal annual compliance review is submitted annually to the DOT CISO.

D.5.5 The cybersecurity-related responsibilities for the role of **OST Information Systems Security Manager (ISSM)** are the same as those of the Component ISSM, as listed in DOT Order 1351.37.5.14.1 – 37.5.14.37.

(Table of Contents)

## D.6 Dates

D.6.1 This OST Cybersecurity Policy is effective as of the date signed.

(Table of Contents)

## D.7 Cancellations

D.7.1 None.

(Table of Contents)

## D.8 Compliance

D.8.1 This Appendix, along with the Departmental Cybersecurity Policy and Compendium, applies to all Secretarial Offices. It incorporates by reference Section 37.8 of the Departmental Cybersecurity Policy; references to DOT Component are hereby replaced with Secretarial Offices.

D.8.2 The Secretarial Offices must comply with and support the implementation of the OST Cybersecurity Program, to include compliance with Federal requirements and programmatic policies, standards, procedures, and information system security controls. Non-compliance with the OST Cybersecurity Policy, Departmental Cybersecurity Policy and its companion Departmental Cybersecurity Compendium, including failure to resolve or report high risk vulnerabilities in a timely manner, must be reported to the appropriate Secretarial Office official for referral to DOT senior management for resolution.

(Table of Contents)

## **D.12 Attachment 1 Authorities and Guidance**

*Refer to Appendix A of DOT Order 1351.37 for a master list of authorities and guidance. Provided below are the authorities and guidance which support the addition of the OST Cybersecurity Policy as an Appendix to the DOT Order:*

- a) IT Governance Guidance, Nitin Pradhan, DOT CIO, 11 June 2010.

## D.13 Attachment 2 Glossary

*Refer to Appendix B of DOT Order 1351.37 for a master glossary of terms. The terms provided below supplement those listed in Appendix B.*

**Business Owner** -- The *business owner* is the spokesperson for the IT service initiative and the owner of the business, functional, and funding requirements for the system/service throughout the business's life cycle, from concept to disposal. The business owner works with various parties depending on the life cycle phase of the business. These phases include Conception, Development, Deployment, Operation, and Phase out/Disposal. (Defined in DOT OCIO Memo "IT Governance Guidance", 11 June 2010)

**Customer** -- A *customer* is the focus and the recipient of a business service. The business system is implemented to address the business needs of the customer. The success of the business system is determined by the value it provides to its customers.

**Service Level Agreement (SLA)** — A *service level agreement* is a written agreement between a service provider and the customer defining key service targets and responsibilities of both parties. SLAs are developed collaboratively and can be established among the stakeholders identified above. A formal written SLA adds value by:

- Forming a joint understanding between a service provider and a customer regarding expectations from their relationship;
- Improving relationship and communication between service provider and customer;
- Ensuring specific and measurable targets are developed;
- Monitoring and improving customer satisfaction;
- Measuring services against targets to aid performance management and demonstrate service achievement; and
- When targets are breached, providing feedback on cause of breach and details of actions taken to prevent recurrence. (Defined in DOT OCIO Memorandum "IT Governance Guidance", 11 June 2010)

**Service Provider** -- The *service provider* is responsible for providing an IT service in accordance with the business owner's requirements, delivering value to the customer, and supporting successful implementation of a customer's business processes. (Defined in DOT OCIO Memo "IT Governance Guidance", 11 June 2010)

## **D.14 Attachment 3 Acronyms**

*Refer to Appendix C of DOT Order 1351.37 for a complete list of acronyms.*

## D.9 Waivers

D.9.1 Compliance with this Policy is mandatory.

D.9.2 Audit procedures are listed in the Departmental Cybersecurity Policy in Section 37.9.2. References to DOT Component in Order 1351.37 are replaced with Secretarial Offices and/or OST.

(Table of Contents)

## D.10 Audit Procedures

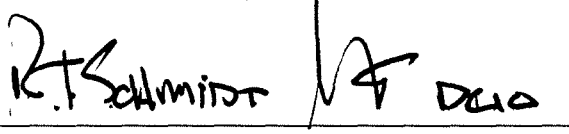
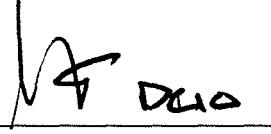
D.10.1 Audit procedures are listed in the Departmental Cybersecurity Policy in Section 37.10.2. References to DOT Component in Order 1351.37 are replaced with Secretarial Offices and/or OST.

D.10.2 This policy will be reviewed on an annual basis alongside of the Departmental Cybersecurity Policy and Compendium.

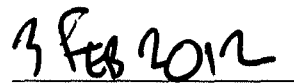
(Table of Contents)

## D.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.

*Mr. Nitin Pradhan*  
*DOT Chief Information Officer*



*Date*

(Table of Contents)