TABLE OF CONTENTS

7.1 What is the purpose of this chapter?

A. This chapter:

(1) Documents security policies supporting relevant Federal laws, regulations, and policies at the Service;

(2) Provides a basis for the information security program;

(3) Supplements the Department of the Interior's Information Technology (DOI IT) Security Policy Handbook;

(4) Is equivalent or more stringent than the Department's policy and standards;

(5) Documents the roles and responsibilities of Service personnel supporting the program;

(6) Designates the major control families associated with information security and defines high-level requirements for those domains; and

(7) Includes specific guidance related to the control families.

B. We will document any deviations from the DOI IT Security Policy Handbook. If a Service policy is less stringent than a Departmental policy, and no documented exception exists, the more stringent Departmental policy is the standard for the Service.

7.2 What is the scope of this chapter? This chapter is applicable to the personnel, contractors, and volunteers who use, operate, plan, secure, and maintain Service-owned information systems.

7.3 What are the authorities for this chapter? In addition to the authorities below, you can review the Department's Cyber Security Division Policy & Guidelines Web site for a more comprehensive list of relevant laws, regulations, and policies**.**

A. Federal information Security Management Act of 2002 (Public Law 107-347).

B. Clinger-Cohen Act (Public Law 104-106).

C. Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources.

D. Computer Fraud and Abuse Act of 1986 (Public Law 99-474).

E. Executive Order 13231, Critical Infrastructure Protection in the Information Age.

F. OMB Circular A-11, Preparation, Submission, and Execution of the Budget; Section 53, Information Technology and E-Government.

G. Presidential Decision Directive 63, Critical Infrastructure Protection.

H. The Department of the Interior Information Technology Security Policy Handbook.

7.4 Who has responsibilities for this program?

A. Senior Leadership: Table 7-1 lists the responsibilities of the Service's senior leadership.

Table 7-1: Information security responsibilities of senior leadership	
These employees…	**Are responsible for…**
(1) Director	**(a)** Delegating responsibility for the overall direction, planning, development, and implementation of the information security program; **(b)** Serving as the Authorizing Official (formerly called the Designated Approval Authority) for certain Service information systems in accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37; and **(c)** Designating a Chief Information Officer (CIO).
(2) Assistant Director – Information Resources and Technology Management (IRTM)	**(a)** Serving as the CIO for the Service; **(b)** Ensuring compliance with Federal information security requirements and the Department's Office of the Chief Information Officer (OCIO) directives; **(c)** Developing and maintaining a Servicewide information security program; **(d)** Developing and maintaining information security policies, procedures, and control techniques to address applicable requirements; **(e)** Ensuring information security control assessments and security authorizations required across the Service are accomplished in a timely and cost-effective manner; **(f)** Ensuring that information security considerations are integrated into acquisition and system life cycles; programming, planning, training, and budgeting cycles; and enterprise architectures; **(g)** Ensuring that the programs designate (in writing) System Security Managers to provide adequate security (see Tables 7-2 and 7-3); **(h)** Designating the Chief Information Security Officer (see Table 7-2); **(i)** Ensuring that employees, contractors, and volunteers receive security awareness briefings and role-based security training (see Table 7-3 for more information); and **(j)** Authorizing the Service-level common controls.
(3) Regional Directors	**(a)** Enforcing applicable information security policies and procedures; **(b)** Ensuring all Regional IT fiscal planning and acquisition for Service-managed information systems comply with information security policies and are integrated into the Capital Planning Investment Control process; **(c)** Consulting with the Chief Information Security Officer to designate a primary and an alternate Regional Information Technology Security Manager; and **(d)** Ensuring information system owners and information system managers are

Table 7-1: Information security responsibilities of senior leadership	
These employees…	**Are responsible for…**
	assigned to information systems in their Regions.

B. Information Security Program Leadership: Table 7-2 lists the responsibilities of the Service's information security program leadership.

Table 7-2: Information security program leadership responsibilities	
These employees…	**Are responsible for…**
(1) Chief Information Security Officer (CISO) ***[Also is the Division Chief, Information Assurance Division, IRTM]***	**(a)** Serving as the point of contact for all Service information security matters; **(b)** Supporting the strategic information security program requirements, including: • Planning and budgeting (Exhibit 300 and Exhibit 53 documents), • Developing internal policy, • Federal Information Security Management Act (FISMA) compliance, and • Compliance with Departmental directives; **(c)** Monitoring the progress of the System Security Managers to ensure they meet program security requirements; **(d)** Working with the Office of the Inspector General (OIG) and incident response team; and **(e)** Overseeing the Servicewide implementation of information security policies, procedures, and guidelines.
(2) Regional IT Security Managers (RITSM)	**(a)** Serving as the points of contact and subject matter experts for Regional information security matters; **(b)** Working in coordination with Chief Technology Officers to implement, disseminate, and monitor Regional compliance with Service security policy and procedures; **(c)** Participating in Regional system development teams and telecommunications planning; **(d)** Coordinating the establishment of Regional common security controls and system security controls to protect information; **(e)** Working with program and IT employees to determine security categorization of information systems; **(f)** Planning security costs for Regional IT investments and systems; and **(g)** Participating in security initiatives including, but not limited to, computer investigations and forensics.

Table 7-2: Information security program leadership responsibilities	
These employees…	**Are responsible for…**
(3) System Security Managers (SSM)	**(a)** Serving as points of contact for end users with security issues related to a specific information system(s); **(b)** Coordinating implementation of system security requirements by evaluating requirements and controls; **(c)** Reporting security costs as part of the Capital Planning and Investment Control process; **(d)** Updating the electronic inventory for system computers; **(e)** Assisting system owners and the Regional Information Technology Security Manager with contingency planning activities; and **(f)** Auditing application, system, and security logs for security threats, vulnerabilities, and suspicious activities in accordance with incident response procedures.

C. Information System Owners, End Users, and their Supervisors: Table 7-3 lists the responsibilities of the Service's information system owners, end users, and their supervisors.

Table 7-3: Responsibilities of information system owners, end users, and their supervisors	
These employees…	**Are responsible for…**
(1) Information System Owners	**(a)** Ensuring that the information systems for which they are responsible—including systems that support the operations and assets of the Service and those that other agencies, contractors, or other sources provide or manage—are compliant with applicable Federal and Departmental guidance, including security requirements; **(b)** Ensuring contractors or employees conduct an information security assessment and authorization on information systems for which they are responsible and providing the necessary system-related documentation to the Branch of Compliance; **(c)** Assigning a System Security Manager for their information systems; **(d)** Ensuring that access to the information system is managed in accordance with Federal and Departmental policies; **(e)** Coordinating security control assessments and authorizations with the Branch of Compliance; and **(f)** Ensuring that the cost of security controls is explicitly identified as part of life-cycle planning of the overall system.
(2) Supervisors of End Users	**(a)** Ensuring that users under their supervision (including contractors and volunteers): • Adhere to the information security policy and procedures in this

Table 7-3: Responsibilities of information system owners, end users, and their supervisors	
These employees…	**Are responsible for…**
	chapter; • Read the Acceptable Use Security Standard, system-specific rules of behavior, and complete a systems operation request before they can access the network; and • Have the requisite information security clearance, training, and access levels appropriate to their duties; **(b)** Reporting employee, volunteer, and contractor transfers and separations that require removal from the system or a change in accounts to the RITSM in accordance with the exit clearance process in 223 FW 13 and 14; **(c)** Reporting incidents that may violate security policy and procedures to the RITSM; and **(d)** Developing position descriptions and performance standards that reference information security responsibilities.
(3) System End Users	**(a)** Completing the applicable access request form and abiding by all rules of behavior associated with an information system; **(b)** Reporting to their supervisors anything they think could be a breach or threat to system security; and **(c)** Completing annual information security training required by the Department.

7.5 What are the standards and requirements the Service has developed to manage the information security program?

A. The Department's and the Service's Information Security control families and requirements are listed in Table 7-4 (NIST defines these control families).

B. The Information Security Program's Branch of Compliance or Division of Information Assurance's Branch of Compliance publishes information security handbooks detailing specific role-based responsibilities on its Intranet site.

Table 7-4: Information Security Control Families and Requirements	
Control Family	**Basic Requirements**
(1) Access Control	Programs/Regions must ensure that: • Processes exist to identify and authenticate users, and • Appropriate permissions are assigned to the user or user group.
(2) Awareness and Training	Service employees must: • Be aware of appropriate use, protection, and security of information; and • Protect the confidentiality, integrity, and availability of information assets, resources, and systems from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption.

Table 7-4: Information Security Control Families and Requirements	
Control Family	**Basic Requirements**
(3) Audit and Accountability	Programs/Regions must: • Use appropriate tools to produce audit trails of user activities, program changes, and record and report program changes; and • Define a process of reviewing those trails to identify any suspicious activities.
(4) Certification, Accreditation, and Security Assessments	Programs/Regions must: • Annually assess the security controls of FISMA-reportable information systems, and • Authorize operation of information systems every 3 years, or whenever the system undergoes significant change.
(5) Configuration Management	Programs/Regions must: • Ensure that information systems comply with established baseline configurations, and • Develop and maintain information security and component inventories, including hardware, software, and firmware.
(6) Contingency Planning	Programs/Regions must: • Establish and maintain test plans for emergency response, backup operations, and post-disaster recovery; and • Test contingency plans at least annually in accordance with contingency planning guidance.
(7) Identification and Authentication	Programs/Regions must: • Identify information system users and processes or devices permitted to access system resources, and • Authenticate (or verify) users or processes before system access is granted.
(8) Incident Response	Programs/Regions must: • Have an operational incident handling capability, and • Track, document, and report incidents to appropriate organizational officials and authorities.
(9) Maintenance	Programs/Regions must: • Ensure that maintenance is performed periodically in accordance with manufacturer's recommendations, and • Ensure that appropriate tools, techniques, and personnel are authorized to perform maintenance.
(10) Media Protection	Service employees must: • Ensure that information system media (both paper and digital) is protected from loss, alteration, or theft; • Limit access to information to authorized users; and • Sanitize or destroy media before it is repurposed or disposed of.
(11) Physical and Environmental Protection	Programs/Regions must: • Limit physical access to information systems, equipment, and operating environments to authorized individuals; and • Protect assets against unauthorized use, theft, environmental hazards, or inadvertent destruction.
(12) Planning	Programs/Regions must: • Employ processes to ensure the confidentiality, integrity, and availability of information; • Maintain system security plans and update them at least annually; and • Ensure that system security plans describe the security controls in place or planned for the information systems.

Table 7-4: Information Security Control Families and Requirements	
Control Family	**Basic Requirements**
(13) Personnel Security	Programs/Regions must employ controls to ensure that: • Personnel (including contractors and other service providers) are trustworthy and meet established security criteria for those positions; • Access of separated employees, contractors, etc. is terminated promptly to prevent unauthorized or malicious access; and • Develop formal sanctions for personnel failing to comply with organizational security policies and procedures.
(14) Risk Assessment	Programs/Regions must ensure that: • Risk assessments are conducted in accordance with applicable NIST guidance; • Risk assessments are updated every 3 years, or whenever there are significant changes to an information system; and • Periodic vulnerability scans of information systems are conducted.
(15) System and Services Acquisition	Programs/Regions must ensure that: • Sufficient resources are allocated to protect information systems, • System development life cycle processes incorporate information security considerations, • Service networks employ software use and installation restrictions, and • Third-party providers employ adequate security measures to protect outsourced information, applications, and services.
(16) System and Communications Protection	Programs/Regions must: • Monitor, control, and protect organizational communications (i.e., information that our systems transmit or receive) at the external boundaries and key internal boundaries of those systems; and • Employ architectural designs, software development techniques, and engineering principles that promote effective information security.
(17) System and Information Integrity	Programs/Regions must: • Employ processes to identify, report, and correct information and information system flaws in a timely manner; and • Protect information systems from malicious code or other vulnerabilities.
(18) Program Management	The Service must ensure that: • Appropriate processes and personnel exist to fund, identify, and track information security deficiencies; and • Up-to-date Service guidance is published related to the protection of information technology resources.

7.6 Can employees get a waiver of information security control requirements for an information system? In some situations it is possible to get a waiver of a requirement(s).

A. To get a permanent waiver of a requirement for an information system, the system owner must use the Department's Plan of Action and Milestone (POA&M) Process Standard. This process involves completing a form that explains the risk and why it's necessary or in the best interest of the Government not to meet the requirement.

B. To get a temporary waiver or a waiver for a single component of an information system, system owners must use the Service's Information Security Control Waiver Form (available on the Intranet).

7.7 Who can you contact for additional information? If you have questions, comments, or concerns about information security or the content of this chapter, contact the Division of Information Assurance. Employees can send comments and questions to the Division through the Intranet by clicking here.

/sgd/ Jeffrey L. Underwood
ACTING DEPUTY DIRECTOR

Date: June 1, 2010