

United States
Department of the Interior

*Revised
file
8/3/2011*



Role-Based Security Training (RBST)
Standard v2.6.0

March 11, 2011

Document Change History

Version Number	Release Date	Summary of Changes	Section Number/ Paragraph Number	Changes Made By
1.0	01/13/2007	Bureau Comments Incorporated	Various	Mikki Smith
1.2	10/05/2007	ITST Staffing of Updated Comments	Various	ITST Training Subcommittee
1.3	01/30/2008	Final Draft for CIO Review/Promulgation	Various	CSD
2.0	7/17/2009	<ul style="list-style-type: none"> • Provided additional detail per NIST SP 800-16 Rev 1 draft • Changed the security training groupings to be consistent with OPM 5 CFR Part 930 • Allowed the maintenance of DOI approved information security certifications to satisfy RBST requirements • Added an enforcement clause for the completion of mandated training • Added Appendices C – E, which should be reviewed and updated each fiscal year 	Various	Lance Kelson
2.1	8/17/2009	Incorporated input from IT SEAT WG and CSD	Various	IT SEAT WG
2.2	8/25/2009	Incorporated input from ITST	1.4	ITST
2.3	9/22/2009	Replaced arbitrary minimum required hours of training annually for each security training group with minimum number of Information Security Training Focus Areas	2.1	Larry Ruffin, Chris Rutherford
2.4	10/2/2009	Final Draft for CIO Review/Promulgation	2.1	Lance Kelson
2.5	11/3/2009	Incorporated input from PAM <ul style="list-style-type: none"> • Define DOI personnel as employees and contractors • Reiterate minimum requirements • Removed language covering financial responsibility for RBST 	1.2 App D 2.3	Lance Kelson
2.5.1	3/11/2010	Incorporated the 'Approved' list of Classes/Focus Areas within App D	App D	FWS: Tyler Marriott, Lan Nguyen BLM: D'Andrea S Spann
2.6.0	3/4/2011	<ul style="list-style-type: none"> • Removed references to Extra Transcript Items and Certification and Accreditation. • Changed RBST artifact retention requirement to 12 months 	2.1	Lance Kelson

TABLE OF CONTENTS

1 INTRODUCTION..... 1

 1.1 BACKGROUND 1

 1.2 PURPOSE..... 1

 1.3 SCOPE..... 2

 1.4 AUTHORITY 2

 1.5 DEFINITIONS..... 4

 1.6 STRUCTURE 4

2 DOI ROLE-BASED SECURITY TRAINING STANDARD 5

 2.1 DOI INFORMATION SECURITY TRAINING GROUPS..... 5

 2.2 ASSIGNING PERSONNEL TO INFORMATION SECURITY TRAINING GROUPS.. 9

 2.3 TRAINING TO CONTRACTORS 10

 2.4 TRAINING CONTENT..... 10

3 DOI ROLE-BASED SECURITY TRAINING, TRACKING AND COMPLIANCE REPORTING..... 11

 3.1 MANAGEMENT AND TRACKING 11

 3.2 COMPLIANCE REPORTING 11

APPENDIX A – ACRONYMS 12

APPENDIX B – REFERENCES 14

APPENDIX C - LISTING OF DOI RECOGNIZED INFORMATION SECURITY PROFESSIONAL CREDENTIALS 15

1 INTRODUCTION

1.1 BACKGROUND

Information Security is a top Department of the Interior (DOI) priority. A strong Departmental IT Security Program (ITSP) cannot be sustained without an investment in training. To be most effective, training must focus on key information security issues such as security policy, procedures, and techniques, as well as the various management, operational, and technical controls necessary and available to secure information resources. Failure to adequately address information security training places the Department's information and information systems at greater than acceptable risk.

Accordingly, the Department has established a comprehensive, measurable, and cost-effective Role-Based Security Training Standard that will enable Bureaus and Offices to strengthen their existing Information Security Training Programs, and thus strengthen the Department's overall ITSP. A robust and Department-wide training program is paramount to ensuring that personnel understand their information security responsibilities, Departmental policies, and how to properly protect information resources entrusted to them.

All levels of personnel have roles to play in the success of the ITSP. However, Bureau/Office Heads, Human Resources Managers, Chief Information Officers (CIO's), Program Managers, Bureau Training Managers, Contracting Officers, and Bureau/Office Chief Information Security Officers (CISO's) have key responsibilities to ensure that an effective program is implemented throughout their Bureaus or Offices.

1.2 PURPOSE

The purpose of the *DOI Role-Based Security Training (RBST) Standard* is to provide Bureaus and Offices with requirements and guidance to enhance their ability to provide appropriate role-based security training for DOI personnel, which includes employees and contractors. The Standard focuses on requirements that are associated with job functions, or roles and responsibilities specific to individuals having significant information security responsibilities. It provides a planning framework to identify training requirements and needs throughout the workforce and ensures that applicable personnel receive appropriate training. This guide provides Bureau/Office Human Resources Managers, contract management staff, supervisors and training administrators with guidance to identify personnel who are required to receive role-based security training, categorize those personnel into appropriate training groups, and report on training compliance for those groups.

1.3 SCOPE

This Standard covers the RBST requirements for all DOI employees and contractors¹ who have elevated privileges or significant information security responsibilities for DOI information systems. Specifically, anyone that manages, acquires, designs and develops, implements and operates, and/or reviews and evaluates any of the NIST SP800-53² security controls has significant information security responsibilities. Such training requirements extend beyond those individuals with direct information system or information security responsibilities. They also encompass those individuals with mission or non-IT program responsibilities, where those responsibilities are supported through the use of information systems such as system owners and Authorizing Officials/Designated Accreditation Authorities.

This standard describes the federal requirements for RBST; identifies key stakeholders responsible for compliance; establishes the minimum DOI requirements for role-based security training based on roles, responsibilities and functions; and defines DOI RBST tracking and reporting criteria. RBST requirements for persons with significant information security responsibilities, including Information Security Basics, are in addition to mandatory annual Federal Information System Security Awareness (FISSA) training.

1.4 AUTHORITY

Federal requirements addressing the role-based security training of DOI personnel are summarized below. These requirements provide the foundational authority for this Standard. For each requirements document identified, a specific citation addressing information security training requirements has been excerpted to identify key responsibilities and training obligations.

- **Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Resources***

“Training. Ensure that all individuals are appropriately trained in how to fulfill their security responsibilities before allowing them access to the system. Such training shall assure that employees are versed in the rules of the system, be consistent with guidance issued by NIST and OPM, and apprise them about available assistance and technical security products and techniques. Behavior consistent with the rules of the system and periodic refresher training shall be required for continued access to the system.”

“Specialized Training”³.ensure that all individuals receive specialized training focused on their responsibilities and the application rules. This may be in addition to the training required for access to a system. Such training may vary from a notification at the time of access (e.g., for members of the public using an information retrieval application) to formal training (e.g., for an employee that works with a high-risk application).”

¹ See Section 2.3 Training to Contractors

² <http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf>

³ The OMB Circular employs the term “Specialized Training” in lieu of “Role-based Security Training” when referring to required supplemental information security training.

- **Federal Information Security Management Act (FISMA), Title III – Information Security**

“...security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of— (A) information security risks associated with their activities; (B) and their responsibilities in complying with agency policies and procedures designed to reduce these risks.”

FISMA requires that the head of each agency *“delegate to the agency Chief Information Officer...the authority to ensure compliance with the requirements imposed on the agency...,including— training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities...”*

- **Office of Personnel Management (OPM), 5 CFR Part 930, *Information Security Responsibilities for Employees Who Manage or Use Federal Information Systems:***

“Each Executive Agency must develop a plan for Federal information systems security awareness and training and

(a) Identify employees with significant information security responsibilities and provide role-specific training in accordance with National Institute of Standards and Technology (NIST) standards and guidance available on the NIST Web site, <http://csrc.nist.gov/publications/nistpubs/>”

- **National Institute of Standards and Technology (NIST) Special Publication 800-16, Revision 1 (Draft) *Information Security Training Requirements: A Role- and Performance-Based Model*⁴**

“FISMA requires agencies to identify and train those personnel with significant responsibilities for information security. These personnel - whether executives, information security program staff members, or system/network administrators - are in positions that are responsible for the security of the organization’s information and information systems. Because of their positions, they can have the greatest positive or negative impact on the confidentiality, integrity, and/or availability of agency information and information systems. Specialized role-based information security training is necessary to help ensure that these “keys to security” clearly understand that information security is an integral part of their job; what the organization expects of them; how to implement and maintain information security controls; mitigate risk to information and information systems; monitor the security condition of the security program, system, application, or information for which they are responsible; and/or what to do when security breaches are discovered. These personnel must:

- *Attend role-based training identified/approved by their management,*
- *Advise their management of additional training that can help them better secure information and information systems for which they are responsible, and*

⁴ This citation is excerpted from Section 1.5.6 “Personnel with Significant Responsibilities for Information Security”. Roles and responsibilities for personnel with significant responsibilities for information security appearing in the final version of SP 800-16, Rev 1 will be the updated corresponding requirement in this standard.

- *Apply what is learned during training.*
- **OPM 5 CFR, Part 410.701(a)(b) - Training; Reporting Requirements**
 - “(a) Each agency shall maintain records of training plans, expenditures, and activities in such form and manner as necessary to submit the recorded data to the Office of Personnel Management (OPM) through the OPM Governmentwide Electronic Data Collection System.*
 - (b) Beginning December 31, 2006, each agency shall report the training data for its employees’ training and development at such times and in such form as required for the OPM Governmentwide Electronic Data Collection System, which is explained in the Guide to Personnel Recordkeeping and the Guide to Human Resources Reporting. ”*
- **Departmental Manual Part 370, Chapter 752 “Discipline and Adverse Actions”, Table of Offenses and Penalties, General Misconduct**
 - “Failure or delay in carrying out instructions; failure or carelessness in performing assigned work; failure to take/complete officially-directed training. ”*
 - *Penalty for First Offense: Written Reprimand to 14-day suspension*
 - *Penalty for Second Offense: 14- to 30- day suspension*
 - *Penalty for Third Offense: 30- day suspension to removal*

1.5 DEFINITIONS

For purposes of this Standard, DOI defines “significant information security responsibility” as any individual whose job role or function includes any of the following:

- Elevated or advanced rights, beyond a general user, to DOI IT systems for information system support and administration purposes;
- Bureau/Office and Departmental officials providing information security program management, oversight, policy, compliance, implementation or information security support responsibilities;
- IT managers and executives providing IT program management, oversight, policy, compliance or implementation responsibilities; and
- Other staff that have functions that impact the implementation, maintenance, or evaluation of cyber security above their own user level.

1.6 STRUCTURE

This standard is organized into three major sections:

- **Section 1: Introduction** – introduces the standard and federal requirements
- **Section 2: DOI Role-Based Security Training Standard** – details departmental mandates and standards for role-based security training; and
- **Section 3: DOI Role-Based Security Training Tracking and Compliance Reporting** - describes the required reporting and tracking processes.

2 DOI ROLE-BASED SECURITY TRAINING STANDARD

2.1 DOI INFORMATION SECURITY TRAINING GROUPS

An analysis of the job functions within DOI Bureaus and Offices, DOI's definition of "significant information security responsibility" in section 1.5 of this Standard, OPM mandates, and the recommendations from NIST has led to the establishment of four role-based training group designations. These groups should be considered a training program starting point. Bureaus and Offices may identify and require that additional roles and functions require RBST. Such determinations should be based on assessed risk or impact and/or operational need. Any additional Bureau- or Office-specific training requirements should be identified in Bureau or Office security documentation (policy or guidance documents) or in the appropriate System Security Plan (SSP).

Each group shall have minimum RBST Requirements. In General:

1. Bureau/Office Heads shall ensure that all personnel identified having significant information security responsibilities receive role-based security training annually.
2. Bureau/Office Training Managers, HR personnel, supervisors, and Bureau/Office CISOs are responsible for collaborating to develop information security training plans for personnel that include the mandated training requirements outlined in this standard. Supervisors, in consultation with the employee, are in the best position to determine individual employee's training needs, consistent with the employee's Performance Appraisal Plan and Individual Development Plan.
3. It is the responsibility of the employee and supervisor, contractor and contract management staff, and the Bureau/Office CISO to ensure that the employee/contractor has sufficient RBST to adequately fulfill the information security responsibilities of his/her assigned role.
4. Bureau/Office Heads will ensure that training plans are established and implemented in accordance with NIST Special Publication 800-16. Emphasis should be placed, to the extent possible, in providing training specifically based on current job roles rather than general Information Security topics.
5. Bureaus and Offices may provide additional, technology specific education and training to employees and contractors via online training, classroom instruction, seminars, or security forums. Since DOI LEARN is the system of record for training for DOI, such training will be recorded in the employee/contractor's DOI LEARN transcript but may not be applicable to RBST requirements unless approved by the BCISO or his/her designate. It is at the discretion of the Bureau or Office to determine the most cost-effective sources for training to meet the training needs of personnel filling supporting information system roles. To the extent practical, Bureaus and Offices shall utilize the Department's on-line centralized solution, DOI LEARN, for any RBST provided to employees/contractors with significant information security roles and responsibilities to enable consistent and effective tracking.

6. Employee RBST completed outside of DOI LEARN shall include creation of an SF 182⁵ entry in DOI LEARN, which must be approved by supervisors. Bureaus and Offices will utilize the SF 182 in DOI LEARN to track and facilitate reporting of RBST costs outside of DOI LEARN for employees.
7. Evidence (e.g. certificates of completion, or professional credential certificates and associated continuing education transcripts) of employee/contractor RBST completed outside of DOI LEARN shall be retained for twelve months after completion of the activity.
8. Bureaus and Offices must coordinate with their appointed DOI LEARN Managers and Data Stewards to ensure that required courses have been assigned to applicable employee/contractors' course lists within DOI LEARN. To determine the DOI LEARN point of contact for each Bureau or Office, visit: <http://www.doi.gov/hrm/DOILearn.html>.
9. In cases where an employee/contractor has multiple roles, and multiple training groups may apply, the training group assignment should be designated based on the training requirements of the employee/contractor's most rigorous job role and function. For example, a senior management official with Information Owners responsibilities who also serves as an Information System Security Officers (ISSO) should be assigned to the Information Security Personnel group, as opposed to the Executive and Senior Management group, based on the more rigorous training requirements of the former.
10. Acquisition and maintenance of a recognized information security professional credential may be substituted for the RBST group requirements described in the sections below. Evidence of these activities related to information security professional credentials must be presented to the BCISO or his/her designate and retained by the contractor/employee. See Appendix C for a listing of DOI recognized information security professional credentials for the current fiscal year.
11. To facilitate tracking of RBST completions, Bureaus and Offices have the option of requiring RBST designated participants to complete a DOI-wide RBST self-certifying course available in DOI LEARN upon completion of their annual RBST requirements to certify they understood and completed their fiscal year RBST requirements. Assertions that RBST requirements have been met by self-certification must be validated by supervisors and are subject to audit by Human Resources, OCIO, and the Office of the Inspector General. Supervisors and managers are responsible for validating that direct reports assigned RBST have completed their annual RBST requirements.

⁵ OPM Memorandum dated July 2, 2007, New Standard Form (SF) 182, Authorization, Agreement and Certification of Training Form

- **Group 1 - Executive and Senior Management**
 - Consists of DOI Senior Executive Level and other senior management personnel whose job functions may include IT management activities that typically extend and apply to an entire organization or major components of an organization. This includes, but is not necessarily limited to, strategic planning, capital planning and investment control, workforce planning, policy and standards development, resource management, knowledge management, architecture and infrastructure planning and management, auditing, and information security management.
 - Group membership includes:
 - Bureau, Regional, and Office IT Division Heads
 - Chief Information Officers (CIOs)
 - Deputy Chief Information Officers (DCIOs)
 - Authorizing Officials (AOs) or Designated Approving/Accrediting Authorities (DAAs)
 - User Representatives
 - Information System Owners
 - Information Owners
 - Information Security Training Focus Areas⁷ – training should include at least 1 of the following:
 - Information Security Basics
 - Policy Level Security Planning and Management
 - Emergency Management and Disaster Recovery
 - Strategic Security Planning or Implementation
 - Risk Management Framework
- **Group 2 - Program and Functional Management –**
 - Consists of DOI personnel whose job functions must incorporate security considerations into lifecycles of systems and programs. This group also includes services support functions such as adding personnel, establishing training and purchasing IT related items.
 - Group membership includes:
 - IT Project/Program Managers
 - Privacy Act Officers
 - Records Management Officials
 - Freedom of Information Act Officials
 - Information Resource Managers
 - Training personnel
 - Human Resources personnel tasked with inducting new personnel
 - If managing any IT related contracts (including personnel), the following collaboration roles also require role-based security training:

⁷ Reference for all training groups focus areas: Office of Personnel Management (OPM) 5 CFR Part 930, Information Security Responsibilities for Employees Who Manage or Use Federal Information Systems.

- Contracting Officers
- Contracting Officer's Representatives or Contracting Officer's Technical Representatives (COR/COTRs)
- Procurement, acquisitions and budget personnel who must know procedures for tracking IT purchases and including IT related clauses in procurements, acquisitions and contracts
- Information Security Training Focus Areas – training should include at least 2 of the following:
 - Information Security Basics
 - Management and Implementation level training in:
 - Security Planning
 - System/Application Security Management
 - System Application Life Cycle Management
 - Risk Management
 - Contingency Planning
 - Account Management and Access Controls
 - Configuration Management and Change Control
 - Data Classification and Records Management
- **Group 3 – Information Security Personnel**
 - Consists of DOI personnel whose job functions may include ensuring, evaluating or certifying the confidentiality, integrity, and availability of systems, networks, and data through planning, managing, assessment, analysis, development, implementation, or maintenance.
 - Group membership includes:
 - Chief Information Security Officers (CISOs)
 - Deputy Chief Information Security Officers (DCISOs)
 - Information Assurance Officers (IAOs)
 - Information System Security Officers (ISSOs)
 - Information System Security Managers (ISSMs)
 - Plan of Actions and Milestones (POA&M) Managers and Coordinators
 - Network Administrators
 - Telecommunications Specialists
 - Database Administrators
 - System/Application Administrators (including Internet protective systems, or email system administrators)
 - Systems Operations Personnel (e.g. Network Operations Centers (NOCs) and Security Operations Centers (SOCs) administrators and managers)
 - Computer Incident Response Team/Center members (CIRT/CIRC personnel, including forensic analysts)
 - Technical Support Personnel (e.g. help desk personnel/administrators and managers)
 - IT Security Auditors, Assessors, and Information Assurance Compliance Officers

- IT Security Policy and Compliance – Auditors, Evaluators and Managers
- Information Security Training Focus Areas – training should include at least 2 of the following:
 - Information Security Basics
 - Security Planning
 - System/Application Security Management
 - System Application Life Cycle Management
 - Risk Management
 - Contingency Planning
 - Incident Response
 - Account Management and Access Controls
 - Configuration Management and Change Control
 - Data Classification and Records Management
- **Group 4 – IT Functional Management and Operations Personnel –**
 - Consists of DOI personnel whose job functions include activities that include the design, development, enhancement, implementation, support, or disposal of information systems.
 - Group membership includes:
 - Computer Hardware/Software Engineers
 - System Designers/Developers
 - Programmers/Systems Analysts
 - Data Center Personnel not listed in Group 3
 - Information Security Training Focus Areas – training should include at least 2 of the following:
 - Information Security Basics
 - Management and Implementation Level Training in:
 - Security Planning
 - System/Application Security Management
 - System Application Life Cycle Management
 - Contingency Planning
 - Risk Management
 - Data Classification and Records Management

2.2 ASSIGNING PERSONNEL TO INFORMATION SECURITY TRAINING GROUPS

Based on the criteria established within this Standard, supervisors, information security management personnel (e.g. Bureau/Office CISOs), Bureau/Office Training Managers, contract management staff, and HR personnel will coordinate assigning personnel to the training group(s) that best correspond to the individual's current job functions and responsibilities. This assignment process must include all applicable individuals that occupy any of the information security roles, responsibilities or functions identified in Section 2.1 of this Standard.

A record of the Information Security Training Group assigned to each relevant individual shall be maintained as a part of the employee's personnel or training record, as appropriate.

For example:

IT System User Name: "John Smith"

Job Function/Role: "DOI LAN Administrator"

DOI Information Security Training Group: "Information Security Personnel (Group 3)"

2.3 TRAINING TO CONTRACTORS

The DOI RBST requirement is applicable to contractors that support DOI information systems, programs, and missions and that meet the criteria in this guide. Where applicable, Bureaus/Office contract management staff should include contract language in any IT related contracts specifying compliance with DOI annual role-based security training requirements. (See DOI Memorandum *Information Technology Security Requirements for Acquisition*, dated 08-18-2004).

2.4 TRAINING CONTENT

RBST must follow the recommended content guidance outlined in the most current version of NIST Special Publication 800-16, *Information Security Training Requirements: A Role- and Performance-Based Model*.

As outlined by NIST, Information Security training is divided into three fundamental training content categories:

- **Laws and Regulations** – The types of knowledge, skills, behaviors, abilities, and competencies relative to the laws and regulations pertaining to information and asset protection that govern IT management and use of information within the Federal Government. These include government-wide requirements such as the Federal Information Security Management Act (FISMA), policy promulgated by the Office of Management and Budget, standards and guidelines disseminated by NIST, as well as policies and procedures specific to a Department or agency;
- **Security Program** – Competencies relative to the establishment, implementation, and monitoring of an Information Security Program within an organization; and
- **System Life Cycle Security** – Competencies relative to the nature of information security needed throughout each phase of a given system's life cycle. NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, identifies five phases in the system life cycle that are typical for an information system: (i) system initiation; (ii) system development and acquisition; (iii) system implementation/assessment; (iv) system operations and maintenance; and (v) system disposal.

Appendix D, RBST Courses by Group, will be updated each fiscal year with available RBST courses within DOI LEARN.

3 DOI ROLE-BASED SECURITY TRAINING, TRACKING AND COMPLIANCE REPORTING

3.1 MANAGEMENT AND TRACKING

Human Resources (HR) within Bureaus and Offices will coordinate with their DOI LEARN Managers and Data Stewards to ensure that employee security training progress is tracked and managed actively within DOI LEARN. Bureau/Office CISOs or designate must review Information Security Training progress reports generated from DOI LEARN to validate the accuracy of those reports before Bureau/Office submission to Cyber Security Division (CSD).

3.2 COMPLIANCE REPORTING

In accordance with Federal regulations referenced in Section 1.4 of this Standard, DOI has a requirement to ensure role-based security training is provided to employees having significant information security responsibilities. The OCIO CSD will examine RBST progress reports from Bureaus and Offices to ensure compliance across the Department, consolidate and report information security training metrics on behalf of the Department.

APPENDIX A – ACRONYMS

This appendix provides a list of acronyms for information security-related terms. It includes those used in this document as well as others of a general nature that may be of interest.

Acronym	Definition
AO	Authorizing Official
BCISO	Bureau Chief Information Security Officer
CISO	Chief Information Security Officer
CFR	Code of Federal Regulations
CIO	Chief Information Officer
COR	Contracting Officer Representative
COTR	Contracting Officer's Technical Representative
CIRT	Computer Incident Response Team
DAA	Designated Approving/Accrediting Authority
DCIO	Deputy Chief Information Officer
DCISO	Deputy Chief Information Security Officer
DoD	Department of Defense
DOI	Department of the Interior
FISMA	Federal Information Security Management Act
HR	Human Resources
IAO	Information Assurance Officer
IT	Information Technology
ITSP	Information Technology Security Program
ISSO	Information System Security Officer
ISSM	Information System Security Manager
KSA	Knowledge, Skills, Abilities

LAN	Local Area Network
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PM	Program Manager
POA&M	Plan of Actions and Milestones
POC	Point of Contact
RBST	Role-Based Security Training
RITSM	Regional IT Security Manager
SDLC	System Development Life Cycle
SOC	Security Operations Center
SP	Special Publication
SSP	System Security Plan

APPENDIX B – REFERENCES

This appendix provides a list of relevant statutes, regulations, directives, and other guidance applicable to Role-Based Security Training. It includes those cited in this document as well as others of a general nature that may be of interest.

Laws and Office of Management and Budget (OMB) Publications

Public Law 107.347, Title III, Federal Information Security Management Act (FISMA) of 2002, December 17, 2002.

Public Law 104-106, Division E, 40 U.S.C. 1401, Information Technology Management Reform Act (ITMRA) of 1996 (Clinger-Cohen Act), February 10, 1996.

OMB Circular A-130, Transmittal Memorandum #4, Management of Federal Information Resources, November 28, 2000.

OMB Memorandum 99-20, Security of Federal Automated Information Resources, June 23, 1999.

National Institute of Standards and Technology (NIST) Special Publications

NIST SP 800-16, Rev. 1 (Draft) Information Technology Security Training Requirements: A Role- and Performance-Based Model, March 2009.

NIST SP 800-50, Building an Information Technology Security Awareness and Training Program, October 2003.

NIST SP 800-53, Rev. 3, Recommended Security Controls for Federal Information Systems and Organizations, Aug 2009.

NIST SP 800-100, Information Security Handbook: A Guide for Managers, October 2006.

Department of the Interior (DOI) Publications

Part 375 Departmental Manual, Chapter 19, Information Technology Security Program, April 15, 2002.

DOI Information Technology Security Policy Handbook.

DOI Memorandum Information Technology Security Requirements for Acquisition, dated 08-18-2004.

Part 370 Departmental Manual, Chapter 752, Discipline and Adverse Actions, December 26, 2006.

Other Publications

OPM 5 CFR Part 930, Information Security Responsibilities for Employees Who Manage or Use Federal Information Systems.

OPM Memorandum dated July 2, 2007, New Standard Form (SF) 182, Authorization, Agreement and Certification of Training Form

OPM 5 CFR Part 410.701(a)(b), Training; Reporting Requirements, Subpart G – Reporting

DoD 8570.01-M, Information Assurance Workforce Improvement Program

APPENDIX C - LISTING OF DOI RECOGNIZED INFORMATION SECURITY PROFESSIONAL CREDENTIALS

- Carnegie Mellon Software Engineering Institute CERT® - Computer Security Incident Handler (CSIH)
- Federated Enterprise Architecture Certification (FEAC) - Certified Enterprise Architect (CEA)
- Information Systems Audit and Control Association (ISACA) Certified Information Systems Auditor (CISA)
- ISACA Certified Information Security Manager (CISM)
- ISACA Certified in Risk and Information Systems Control (CRISC)
- International Information Systems Security Certification Consortium (ISC)² Certification and Accreditation Professional (CAP)
- (ISC)² Systems Security Certified Practitioner (SSCP)
- (ISC)² Certified Information Systems Security Professional (CISSP)
- (ISC)² Certified Secure Software Lifecycle Professional (CSSLP)
- ASIS International Certified Protection Professional (CPP)
- ASIS International Professional Certified Investigator (PCI)
- ASIS International Physical Security Professional (PSP)

Note: These Information Security Professional Credentials were selected for their relevance to Information Security, and their associated annual continuing education requirements for maintenance of these credentials. Suggestions for adding other credentials to this list can be directed to: [DOI IT Security Training@ios.doi.gov](mailto:DOI_IT_Security_Training@ios.doi.gov).

Group 1 - Executive and Senior Management (Minimum 1 per year)

Focus Areas in Blue

To change the Focus Area simply modify Column B with a different number, 1-10, and 'Sort' on Column 'B' only.

- 1 Information Security Basics
- 1 • Non-SkillSoft / no-charge: 2010 Computer Security Incident Response Training (CSIRT) Overview (1 hr)
- 1 • Protecting and Sharing Excel 2007 Workbooks, mo_expu_a02_dt_enu (2 hrs)
- 1 • Introduction to information security, 216913_ENG (1.75 hrs)
- 1 • Operational information security, 217983_ENG (1.5 hrs)
- 1 • Malicious code and information security, 217043_ENG (1.75 hrs)
- 1 • Information security and the Internet, 216960_ENG (1.5 hrs)
- 2 Policy Level Security Planning and Management
- 2 • Information Security Governance: Overview, sp_cism_a01_it_enu (2 hrs)
- 2 • Information Security Governance: Strategies and Goals, sp_cism_a02_it_enu (2 hrs)
- 2 • Information Security Governance: Developing an Action Plan, sp_cism_a03_it_enu (2 hrs)
- 2 • Information Security Program Development: Introduction and Roadmap, sp_cism_a06_it_enu (2 hrs)
- 2 • Information Security Program Development: Resources, sp_cism_a07_it_enu (2 hrs)
- 2 • Information Security Program Development: Metrics and Implementation, sp_cism_a08_it_enu (2 hrs)
- 2 • Information Security Program Development: Introduction and Framework sp_cism_a09_it_enu (2 hrs)
- 2 • Information Security Program Development: Resources and Implementation, sp_cism_a10_it_enu (2.5 hrs)
- 3 Emergency Management and Disaster Recovery
- 3 • Business Continuity and Disaster Recovery Planning, 244085 (140 mins)
- 4 Strategic Security Planning or Implementation
- 4 • Information Availability, 240092 (2.5 hrs)
- 5 Risk Management Framework
- 5 • Information Risk Management: Program Framework and Risk Assessment, sp_cism_a04_it_enu (2 hrs)
- 5 • Information Risk Management: Analysis, Mitigation, and Monitoring, sp_cism_a05_it_enu (2 hrs)
- 5 • Approaches to Risk Management, PD0242 (2 hrs)
- 5 • Risk Basics, PD0241 (2 hrs)
- 5 • Decisions and Risk, PD0243 (2 hrs)
- 5 • Risk Assessment and Prevention (HRCI/PHR - 2007-aligned), HR0277 (2.5 hrs)
- 5 • Strategic Planning and Risk Management, PD0244 (2.5 hrs)
- 5 • Risk Strategies: The Cutting Edge, PD0245 (2.5 hrs)
- 5 • Strategic Approaches to Risk Management (HRCI/SPHR - 2007-aligned) (2 hrs)
- 5 • Information Security and Risk Management, 243962_ENG (3 hrs)