

1. PURPOSE

The purpose of this document is to establish policy for mandatory training for Department of Commerce (DOC) individuals with significant information system security responsibilities. The intent of this policy is to aid in developing professional competence and to ensure consistent training and subsequent consistent reporting for the significant information security roles within DOC.

2. BACKGROUND

The information system security workforce is critical to assuring that the DOC has adequate security measures to protect and defend its information and information systems. The workforce must be capable of appropriately reporting and responding to suspicious activities, and know how to protect the information and information technology (IT) systems to which they have access. DOC is committed to improving its information system security workforce to ensure the safeguard of its technological assets, and ensure the confidentiality, integrity, and availability of information DOC is entrusted to protect, through a “centralized policy and strategy, distributed implementation” model¹ as its approach to information system security training.

3. SCOPE

The requirements set forth in this policy applies to all Operating Units (OUs) and employees (federal and contractor), guest researchers, collaborators, and others who have a role deemed significant in terms of information system security. The DOC Office of Security (OSY) prescribes the requirements for training regarding the handling of electronic and hard copy national security information. National security training is supplemental to the training requirements set forth herein.

4. AUTHORITY

The DOC Chief Information Officer (CIO) has the authority to develop, implement, and manage information system security processes and procedures to protect the availability, confidentiality, and integrity of the Department's IT resources. The DOC Chief Information Security Officer (CISO) shall ensure that IT security policy and requirements are developed consistent with applicable statutory authority, including the Clinger-Cohen Act and the Federal Information Security Management Act (FISMA); with regulatory requirements and external guidance, including Office of Management and Budget (OMB) policy and Federal Information Processing Standards (FIPS) publications promulgated by the National Institute of Standards and Technology (NIST); and with internal policies and requirements.

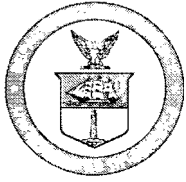
5. CANCELLATION/AUGMENTATION

This CITR replaces Section 4.2.2 and augments Section 4.2.3 in the *U.S. Department of Commerce IT Security Program Policy (ITSPP)*, January 2009.

6. POLICY

Operating Units (OUs) have 180 days from the signature date to implement this CITR. This CITR specifies requirements for Information System Security Training for those personnel with a role deemed herein to be “significant” in terms of information system security responsibilities.

¹ Model 2 defined in NIST Special Publication 800-50, Building an Information Technology Security Awareness and Training Program.



Role Identification and Minimum Hours:

The table below defines the DOC roles deemed to have significant information system security responsibilities. Personnel, to whom these roles are assigned, are required to participate in the corresponding minimum number of training hours for that role, per fiscal year, or provide verification that a role-related, role-approved professional certification has been met or is being maintained.

Significant Role	Annual Requirement
Chief Information Officer (CIO)	1 hour
Authorizing Official (AO)	1 hour
Information System Owner (ISO)	2 hours
Senior Agency Information Security Officer (SAISO) Chief Information Security Officer (CISO) Information Technology Security Officer (ITSO)	Professional certification
Certification Agent (CA)	Professional certification
Information System Security Officer (ISSO)	Professional certification
Key Contingency Roles: Disaster Recovery Coordinator Contingency Plan Coordinator	4 hours
Information System Security Incident Responder	Professional certification

Since there are numerous management, technical, and operational roles that include elements of information security, each DOC Operating Unit (OU) is encouraged to define and track additional roles based on need and/or specific areas that require skill enhancement.

Appendix A provides a mapping of roles defined herein to those defined in *NIST Special Publication 800-37, Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Life Cycle Approach*. Upon DOC requiring the use of Revision 1, the table above will be revised to reflect the new titles for these roles as identified in NIST SP 800-37, Revision 1.

Multiple and/or Duplicative Roles:

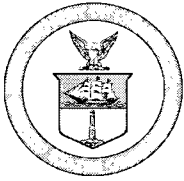
If an individual has multiple significant roles, training should be completed for each role. If the provided training and/or professional certification(s) is duplicative, only one instance of the role-related, role-approved training and/or professional certification is required.

Type of Training

The type of training and/or professional certification required is defined by the DOC and/or OU Office of the Chief Information Officer (OCIO). Appendix C provides a listing of role-related, role-approved web-based courseware which may be used to meet these requirements. These courses may be reviewed annually by the DOC OCIO. Each DOC OU CIO may further define and provide web-based courseware and/or instructor-led training.

Professional Certifications:

Meeting professional certification requirements usually requires a combination of formal training, including continuing education, and experiential activities such as on-the-job training. DOC personnel who successfully complete and maintain a role-related, role-approved professional certification as defined



in Appendix C are considered to have appropriately demonstrated their competence to perform the functions of their assigned “significant” role. Successful accomplishment and maintenance of a role-related, role-approved professional certification is required as indicated in the aforementioned table.

Personnel in these roles that have not met certification requirements must meet with their supervisors to establish a development plan leading to successful accomplishment of a role-related, role-approved professional certification. The associated AO and/or ISO must establish a Plan of Action & Milestone (POA&M) to document the security risk to the information system to which the individual is assigned, from their not having completed certification requirements.

Role-related, role-approved industry professional certifications may be reviewed annually by the DOC OCIO. While the requirement for professional certification is for the aforementioned roles, DOC OU CIOs may extend the requirement to other roles deemed as significant, at their discretion.

Acceptance of other information security-related industry professional certifications is at the discretion of each DOC OU CIO, so long as the professional certification meets the following criteria: (1) is security-related; (2) is accredited (and accreditation maintained) under ISO/IEC 17024²; and (3) has training requirements for maintenance.

Simulated Events or Tabletop Exercises

At the discretion of each DOC OU, simulated events or tests may be used to satisfy the refresher training requirements for Key Contingency Roles, but such tests must be documented as defined by the OU CIO.

Role Notification:

Initial role appointment notification must be made, either in writing or via email, within the first thirty (30) business days of appointment. Appendix B provides sample text that may be used for written or email notification.

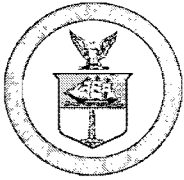
Mandatory language for existing critical elements (collateral duties) and stand-alone elements for employees in these significant roles must be included in performance plans.

Tracking and Reporting

Each OU shall track information security training completion for personnel by documenting the name, role, type of training received, and when training was accomplished or date professional certification was verified. See HR Bulletin #076, FY 08 on requirements to record training in the Commerce Learning Center.

If applicable, it is the responsibility of the personnel to maintain a professional certification and provide verification or proof of certification to the OU OCIO. Personnel must agree to release professional certification qualification(s) to DOC in order to validate successful accomplishment.

² International Standards Organization/International Electronics Commission (ISO/IEC) 17024, “General Requirements for Bodies Operating Certification of Persons,” April 2003.



Training for the roles defined herein must be reported by the OU when submitting FISMA data to DOC. Other OU-defined roles must be tracked by the OU but need not be reported to DOC.

Enforcement and/or Compliance

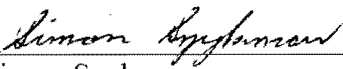
At a minimum, if an employee or associate refuses to engage in, or cannot meet the training and/or professional certification requirements, access to information and resources and their continued performance in the aforementioned role must be re-evaluated, and a risk-based decision made by the Authorizing Official.

Inherently Governmental Roles

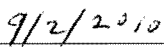
The DOC considers the following roles inherently governmental³, and therefore these roles should not be filled by a non Federal government employee: (1) Chief Information Officer, (2) Authorizing Official, and (3) Senior Agency Information Security Officer (SAISO)/Chief Information Security Officer (CISO)/Information Technology Security Officer (ITSO).

Implementation

For existing employees, requirements contained herein must be provided and maintained by DOC and/or OUs at no cost to government employees. Department Administrative Order (DAO) 202-410, Section 8 titled, Payment of Training Expenses, provides guidance on payment by DOC of expenses to obtain professional credentials and organizational membership, and for continued service requirements. For prospective employees, professional certification requirements for the required roles must be included as a condition of employment. Requirements contained herein must be included in future vacancy announcements for these roles. For associates, agreement or contractual language must specify requirements defined herein. Existing employment agreements or contracts must be modified to specify certification requirements, and to include validation of training and/or professional certification.

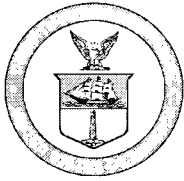


Simon Szykman
Chief Information Officer



Approval Date

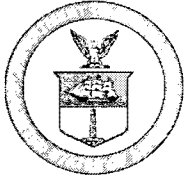
³ These determinations are based on Office of Management and Budget Circular No. A-76, Attachment A § B.



Appendix A: Mapping of Roles to NIST Special Publication 800-37, Revision 1

Appendix A provides a mapping of roles defined herein to those defined in NIST Special Publication 800-37, Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Life Cycle Approach.

Significant Role	Mapped to SP 800-37 Revision 1
Chief Information Officer (CIO)	Chief Information Officer
Authorizing Official (AO)	Authorizing Official or Designated Representative Risk Executive (Function)
Information System Owner (ISO)	Information System Owner Information Owner / Steward Common Control Provider
Senior Agency Information Security Officer (SAISO) Chief Information Security Officer (CISO) Information Technology Security Officer (ITSO)	Senior Information Security Officer
Certification Agent (CA)	Security Control Assessor
Information System Security Officer (ISSO)	Information System Security Officer Information Security Architect Information System Security Engineer
Key Contingency Roles: Disaster Recovery Coordinator Contingency Plan Coordinator	Not referenced
Information System Security Incident Responder	Not referenced



Appendix B: Sample Notification Text

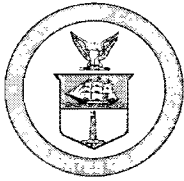
INITIAL ROLE AND TRAINING NOTIFICATION

Subject: Appointment of *[role name]*

This serves as notification that you are hereby appointed to the role of *[role name]* for *DOC Information System(s) numbered [list number(s)]*. This role is deemed significant in terms of information system security (ISS), and requires *[required number of hours or accomplishment/validation of a role-related role-approved professional certification]*, annually based on fiscal year.

[Describe available training and where to access]

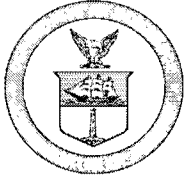
Your designation shall remain in effect through the life of the system unless notified of a change in designation in writing by the system's Authorizing Official and/or Information System Owner. If you have any questions regarding training, or feel there is an error in your designated responsibility, please contact your OU Information Technology Security Officer.



Appendix C: Role-Related, Role-Approved Professional Certifications and Commerce Learning Center (CLC) Courseware

*Each role deemed as significant in terms of information system security has a mapping to a role-related, role-approved **professional certification**. Note that professional certification are not required for all roles, but are listed as a guide in cases where they are not mandatory. Note that certifications for required roles are aligned with the latest Department of Defense 8570.01-M, change 2 (April 2010).*

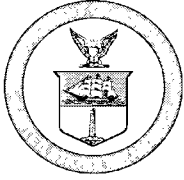
*Role-related, role-approved **web-based training courses** are listed by the course name and course number. Web-based courseware considers three fundamental training content categories as defined by NIST Special Publication 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model. All courses listed are available via the Commerce Learning Center (CLC) in web-based format, and have been purchased for use by DOC. Each OU's Training Officer can provide information on licensing and duration of access for the CLC and course library (SkillSoft). DOC OCIO may review each August, the web-based training offerings and professional certifications to ensure continued relevance. Thereafter, each OU should implement changes within the Learn Center for changes to take affect at the beginning of the new performance cycle (fiscal year).*



ROLE	Annual Requirement
DOC and OU Chief Information Officer (CIO)	1 hour
<i>Web-based Course Name and Number⁴</i>	
Project Management for IT Professionals	
Project IT Management Simulation - The Early Stages	PROJ0350
Functions of IT Project Management	PROJ0352
The Life Cycle of an IT Project	PROJ0353
Managing the Execution and Control of IT Projects	PROJ0354
Managing Efficiencies of IT Projects	PROJ0355
Project IT Management Simulation - Design to Rollout	PROJ035S
Strategic Project Management for IT Projects	
Strategic Project Management for IT Projects Simulation	PROJ0360
Strategic Planning and Positioning for IT Projects	PROJ0361
Strategic Approaches to Managing IT Projects	PROJ0362
Estimating the IT Project Work Effort	PROJ0363
IT Project Leadership, Authority & Accountability	PROJ0364
Managing Multiple IT Projects	PROJ0365
Cost Management and IT Project Trade-offs	PROJ0366
Project Risk Management (PMBOK® Guide - Third Edition-aligned)	
Planning and Identifying Project Risk	PROJ0591
Analyzing Project Risk	PROJ0592
Responding to and Controlling Project Risk	PROJ0593
<i>Optional role-related, role-approved Professional Certifications⁵</i>	
GIAC Information Security Fundamentals (GISF)	
GIAC Security Leadership Certification (GSLC)	
CompTIA Security+	
(ISC) ² Certified Authorization Professional (CAP)®	
ISACA® Certified Information Security Manager (CISM)®	
(ISC) ² Certified Information System Security Professional (CISSP)® or Associate	

⁴ SkillSoft Job Role/Competency Mappings for CIO, SecRole-mapping updated 092809.xls

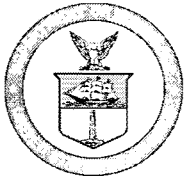
⁵ Maps to DoD 8570.01-M, Change 2 (April 2010). IAM Levels I, II, and III



ROLE	Annual Requirement
Authorizing Official (AO)	1 hour
<i>Web-based Course Name and Number⁶</i>	
Information System Security	
Systems Security Engineering	206760_ENG
Certified Information Systems Security Professional (CISSP)	TPCISSP_ENG
The Information Systems Security Engineering Professional (ISSEP) Domains	
Systems Security Engineering	206760_ENG
Certification and Accreditation	206761_ENG
Industry Overviews	
Industry Overview: Federal Government	indo_02_a12_bs_enus
<i>Optional role-related, role-approved Professional Certifications⁷</i>	
GIAC Information Security Fundamentals (GISF)	
GIAC Security Leadership Certification (GSLC)	
CompTIA Security+	
(ISC) ² Certified Authorization Professional (CAP)®	
ISACA® Certified Information Security Manager (CISM)®	
(ISC) ² Certified Information System Security Professional (CISSP)® or Associate	

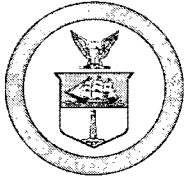
⁶ SkillSoft Job Role/Competency Mappings for DAA, SecRole-mapping_updated 092809.xls

⁷ Maps to DoD 8570.01-M, Change 2 (April 2010). IAM Levels I, II, and III



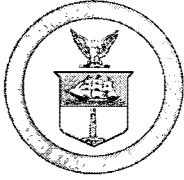
ROLE	Annual Requirement
Information System Owner (ISO)	2 hours
<i>Web-based Course Name and Number⁸</i>	
The Certified Information Systems Security Professional (CISSP) Domains	
CISSP Domain: Information Security and Risk Management	243962_ENG
CISSP Domain: Security Architecture and Design	243975_ENG
CISSP Domain: Access Control	243986_ENG
CISSP Domain: Application Security	243998_ENG
CISSP Domain: Operations Security	244020_ENG
CISSP Domain: Cryptography	244031_ENG
CISSP Domain: Physical (Environmental) Security	244059_ENG
CISSP Domain: Telecommunications and Network Security	244069_ENG
CISSP Domain: Business Continuity and Disaster Recovery Planning	244085_ENG
CISSP Domain: Legal, Regulations, Compliance and Investigations	244096_ENG
The Information Systems Security Engineering Professional (ISSEP) Domains	
Systems Security Engineering	206760_ENG
Certification and Accreditation	206761_ENG
Technical Management	206762_ENG
US Government Information Assurance Regulations	206763_ENG
Industry Overviews	
Industry Overview: Federal Government	indo_02_a12_bs_enus
Project Management	
Managing the Execution and Control of IT Projects	PROJ0354
Estimating the IT Project Work Effort	PROJ0363
Integrated Project Change Control and Close	proj_06_a03_bs_enus
Executing, Monitoring & Controlling, and Closing a Project	PROJ0515
Integrated Project Execution, Monitoring, and Control	proj_06_a02_bs_enus
Project Integration: Executing and Completing a Project	PROJ0522
Monitoring and Controlling Project Scope	proj_07_a03_bs_enus
Controlling Project Scope	PROJ0532
Risk Response, Monitor, and Control	proj_13_a03_bs_enus
Responding to and Controlling Project Risk	PROJ0593
Statistical Process Control (SPC) in Six Sigma	oper_18_a01_bs_enus
Sustaining Improvements and Gains from Six Sigma Projects	oper_18_a03_bs_enus
Lean and Six Sigma	oper_11_a01_bs_enus
Six Sigma Projects and the Black Belt Role	oper_11_a02_bs_enus
Six Sigma Leadership and Change Management	oper_11_a03_bs_enus
Probability for Six Sigma	oper_15_a05_bs_enus
<i>Optional role-related, role-approved Professional Certifications⁹</i>	

⁸ SkillsSoft Job Role/Competency Mappings for System Owner, SecRole-mapping_updated 092809.xls



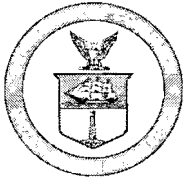
GIAC Information Security Fundamentals (GISF)
GIAC Security Leadership Certification (GSLC)
CompTIA Security+
(ISC)² Certified Authorization Professional (CAP)[®]
ISACA[®] Certified Information Security Manager (CISM)[®]
(ISC)² Certified Information System Security Professional (CISSP)[®] or Associate

⁹ Maps to DoD 8570.01-M, Change 2 (April 2010). IAM Levels I, II, and III



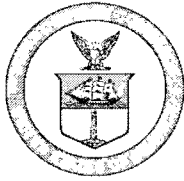
ROLE	Annual Requirement
DOC and OU Senior Agency Information Security Officer (SAISO), Chief Information Security Officer (CISO), or Information Technology Security Officer (ITSO)	professional certification
<i>Web-based Course Name and Number¹⁰</i> <i>(may be used in support of Certification continuing education and/or maintenance credits)</i>	
The Certified Information Systems Security Professional (CISSP) Domains	
CISSP Domain: Information Security and Risk Management	243962_ENG
CISSP Domain: Security Architecture and Design	243975_ENG
CISSP Domain: Access Control	243986_ENG
CISSP Domain: Application Security	243998_ENG
CISSP Domain: Operations Security	244020_ENG
CISSP Domain: Cryptography	244031_ENG
CISSP Domain: Physical (Environmental) Security	244059_ENG
CISSP Domain: Telecommunications and Network Security	244069_ENG
CISSP Domain: Business Continuity and Disaster Recovery Planning	244085_ENG
CISSP Domain: Legal, Regulations, Compliance and Investigations	244096_ENG
The Information Systems Security Engineering Professional (ISSEP) Domains	
Systems Security Engineering	206760_ENG
Certification and Accreditation	206761_ENG
Technical Management	206762_ENG
US Government Information Assurance Regulations	206763_ENG
CompTIA Security+ 2008 (or later)	
CompTIA Security+ 2008: Threat Mitigation	cs_sety_a01_it_enus
CompTIA Security+ 2008: Cryptography	cs_sety_a02_it_enus
CompTIA Security+ 2008: Authentication Methods	cs_sety_a03_it_enus
CompTIA Security+ 2008: Messaging, User, and Role Security	cs_sety_a04_it_enus
CompTIA Security+ 2008: Public Key Infrastructure and Access Security	cs_sety_a05_it_enus
CompTIA Security+ 2008: Ports, Protocols, and Network Security	cs_sety_a06_it_enus
CompTIA Security+ 2008: Wi-Fi and Remote Access	cs_sety_a07_it_enus
CompTIA Security+ 2008: Risk Analysis, Vulnerability Testing, IDS, and Forensics	cs_sety_a08_it_enus
CompTIA Security+ 2008: Auditing, Security Policies, and Disaster Recovery	cs_sety_a09_it_enus
CompTIA Security+	
General Security Concepts	84869_ENG
Communications Security	84870_ENG
Infrastructure Security	84871_ENG
Encryption Technologies	65873_ENG
Operational and Organizational Security	84873_ENG

¹⁰ SkillSoft Job Role/Competency Mappings for SAISO, SecRole-mapping_updated 092809.xls



ECDL/ICDL 4 Module 1: Concepts of Information Technology (IT)
ECDL/ICDL 4 Module 1: Concepts of Information Technology (IT) - IT in Daily Life 208426 ENG
<i>Role-related, role-approved Professional Certifications¹¹ (accomplishment/maintenance of one required)</i>
GIAC Information Security Fundamentals (GISF) GIAC Security Leadership Certification (GSLC) CompTIA Security+ (ISC) ² Certified Authorization Professional (CAP)® ISACA® Certified Information Security Manager (CISM)® (ISC) ² Certified Information System Security Professional (CISSP)® or Associate

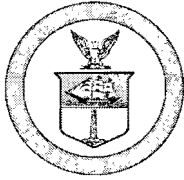
¹¹ Maps to DoD 8570.01-M, Change 2 (April 2010). IAM Levels I, II, and III



ROLE	Annual Requirement
Certification Agent	professional certification
<i>Web-based Course Name and Number¹²</i> <i>(may be used in support of Certification continuing education and/or maintenance credits)</i>	
Auditing: A Practical Approach	
Introduction to Internal Auditing	FIN0232
Introduction to External Auditing	FIN0234
<i>Role-related, role-approved Professional Certifications¹³</i> <i>(accomplishment/maintenance of one required)</i>	
ISACA Certified Information Systems Auditor® (CISA)	
GIAC Systems and Network Auditor (GSNA)	
Electronic Commerce Council Certified Ethical Hacker (CEH)	

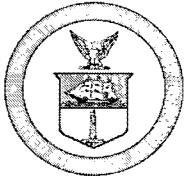
¹² SkillSoft Job Role/Competency Mappings for Computer Audit Specialist, SecRole-mapping_updated 092809.xls

¹³ Maps to DoD 8570.01-M, Change 2 (April 2010), CND Auditor



ROLE	Annual Requirement
Information System Security Officer (ISSO)	professional certification
<i>Web-based Course Name and Number¹⁴</i>	
<i>(may be used in support of Certification continuing education and/ or maintenance credits)</i>	
The Certified Information Systems Security Professional (CISSP) Domains	
CISSP Domain: Information Security and Risk Management	243962_ENG
CISSP Domain: Security Architecture and Design	243975_ENG
CISSP Domain: Access Control	243986_ENG
CISSP Domain: Application Security	243998_ENG
CISSP Domain: Operations Security	244020_ENG
CISSP Domain: Cryptography	244031_ENG
CISSP Domain: Physical (Environmental) Security	244059_ENG
CISSP Domain: Telecommunications and Network Security	244069_ENG
CISSP Domain: Business Continuity and Disaster Recovery Planning	244085_ENG
CISSP Domain: Legal, Regulations, Compliance and Investigations	244096_ENG
The Information Systems Security Engineering Professional (ISSEP) Domains	
Systems Security Engineering	206760_ENG
Certification and Accreditation	206761_ENG
Technical Management	206762_ENG
US Government Information Assurance Regulations	206763_ENG
CompTIA Security+ 2008 (or later)	
CompTIA Security+ 2008: Threat Mitigation	cs_sety_a01_it_enus
CompTIA Security+ 2008: Cryptography	cs_sety_a02_it_enus
CompTIA Security+ 2008: Authentication Methods	cs_sety_a03_it_enus
CompTIA Security+ 2008: Messaging, User, and Role Security	cs_sety_a04_it_enus
CompTIA Security+ 2008: Public Key Infrastructure and Access Security	cs_sety_a05_it_enus
CompTIA Security+ 2008: Ports, Protocols, and Network Security	cs_sety_a06_it_enus
CompTIA Security+ 2008: Wi-Fi and Remote Access	cs_sety_a07_it_enus
CompTIA Security+ 2008: Risk Analysis, Vulnerability Testing, IDS, and Forensics	cs_sety_a08_it_enus
CompTIA Security+ 2008: Auditing, Security Policies, and Disaster Recovery	cs_sety_a09_it_enus
CompTIA Security+	
General Security Concepts	84869_ENG
Communications Security	84870_ENG
Infrastructure Security	84871_ENG
Encryption Technologies	65873_ENG
Operational and Organizational Security	84873_ENG
ECDL/ICDL 4 Module 1: Concepts of Information Technology (IT)	
ECDL/ICDL 4 Module 1: Concepts of Information Technology (IT) - IT in Daily Life	208426_ENG

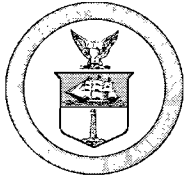
¹⁴ SkillSoft Job Role/Competency Mappings for SAISO, SecRole-mapping_updated 092809.xls



*Role-related, role-approved Professional Certifications¹⁵
(accomplishment/maintenance of one required)*

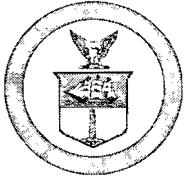
CompTIA A+
CompTIA Network+
(ISC)² Systems Security Certified Practitioner (SSCP)[®]
GIAC Security Essentials Certification (GSEC)
CompTIA Security+
Security Certified Program Security Certified Network Professional (SCNP)
ISACA[®] Certified Information System Auditor (CISA)[®]
GIAC Security Expert (GSE)
Security Certified Program Security Certified Network Architect (SCNA)
(ISC)² Certified Information System Security Professional (CISSP)[®] or Associate
GIAC Certified Incident Handler (GCIH)

¹⁵ Maps to DoD 8570.01-M, Change 2 (April 2010). IAT Levels I, II, and III



ROLE	Annual Requirement
Key contingency roles	4 hours
<i>Web-based Course Name and Number¹⁶</i>	
Storage Technology Foundations	
Introduction to Storage Technology	240031_ENG
Storage System Architecture	240039_ENG
Physical Disks and RAID Arrays	240047_ENG
Intelligent Storage Systems	240056_ENG
Network Storage Systems	240062_ENG
Fiber Channel Storage Attached Networks	240072_ENG
IP SANs and Content Addressed Storage	240082_ENG
Information Availability	240092_ENG
Replication and Business Continuity	241020_ENG
Monitoring and Managing the Data Center	241031_ENG
Securing Storage	254190_ENG
Storage Virtualization Technologies	254207_ENG
<i>Optional role-related, role-approved Professional Certifications</i>	
DRI® Associate Business Continuity Professional (ABCP)	
DRI® Certified Functional Continuity Professional (CFCP)	
DRI® Certified Business Continuity Professional (CBCP)	
DRI® Master Business Continuity Professional (MBCP)	

¹⁶ SkillSoft IT Courseware selected from DOC-Jan2010 catalog.xls



ROLE	Annual Requirement
Incident Responder	professional certification
<i>No existing web-based courseware maps to this role.</i>	
<i>Role-related, role-approved Professional Certifications¹⁷</i> <i>(accomplishment/maintenance of one required)</i>	
GIAC Certified Incident Handler (GCIH) CERT® Certified Computer Security Incident Handler (CSIH) Electronic Commerce Council Certified Ethical Hacker (CEH)	

¹⁷ Maps to DoD 8570.01-M, Change 2 (April 2010). CND Incident Reporter