

NOAA/NESDIS

IT Security Training Policy and Procedures

September 28, 2012



Prepared by:

**U.S. Department of Commerce
National Oceanic and Atmospheric Administration (NOAA)
National Environmental Satellite, Data, and Information Service (NESDIS)**

Table of Contents


Record of Changes/Revisions	5
1.0 Background and Purpose	6
2.0 Scope	6
3.1 Roles, Responsibilities, and Coordination.....	6
3.2 Chief Information Officer (CIO)	7
3.3 Authorizing Official (AO), co-AOs, and AO Designated Representatives (AODRs).....	7
3.4 System Owner (SO).....	7
3.5 Information Technology Security Officer (ITSO) including Alternate ITSOs and direct support staff.....	7
3.6 Information System Security Officer (ISSO) Including Alternate ISSOs and Direct Support Staff	8
3.7 Certification Agent (CA).....	8
3.8 Information Owners (IO).....	8
3.9 Key Contingency Roles.....	8
3.10 Other Significant IT Security Roles as Defined by the SO.....	9
4.0 Management Commitment.....	9
5.1 Compliance.....	9
5.2 References.....	9
6.1 Policy.....	10
6.2 Policy Maintenance.....	10
6.3 Policy Feedback Process.....	10
6.4 Policy Effective Date.....	10
7.1 Procedures for NESDIS Personnel with Significant IT Security Roles	10
7.2 Baseline IT Security Training Procedures	10
7.2.1 Online NESDIS Training.....	11
7.2.2 Laws, Regulations, and Guidance	11
7.3 Role-Based Annual Refresher Training	13
7.3.1 Role Identification and Required Minimum Training Hours	14
7.4 Role-Based Professional Certifications	15
8.1 IT Security Training Program Management Procedures for SOs and the ITSO	18
8.3 Reporting and Tracking.....	18
8.4 Record Retention.....	18



UNITED STATES DEPARTMENT OF COMMERCE
National Oceanic and Atmospheric Administration
NATIONAL ENVIRONMENTAL SATELLITE DATA AND
INFORMATION SERVICE
Siler Spring, Maryland 20910

September 30, 2012

MEMORANDUM FOR: Distribution

FROM: Catrina D. Purvis 
NESDIS Chief Information Officer (Acting)

SUBJECT: Issuance of Updated NESDIS Information Technology
Security Policies and Procedures

This is to announce the issuance of ten updated NESDIS publications for implementing effective, compliant, and consistent information technology (IT) security practices within NESDIS. These documents highlight the specific steps necessary to ensure effective NESDIS implementation. Specifically issued under this memorandum are the

1. NESDIS *Federal Information Processing Standard 199 Security Categorization Policy and Procedures*, v3.0;
2. NESDIS *Plan of Action and Milestones Management Policy and Procedures*, v2.0;
3. NESDIS *Policy and Procedures for Determining Minimum Documentation Requirements for System/Interconnections*, v2.1;
4. NESDIS *Contingency Planning Policy and Procedures*, v2.1;
5. NESDIS *Policy and Procedures for Ensuring Security in NESDIS IT Systems and Services Acquisitions*, v2.1;
6. NESDIS *Security Assessment Report Policy and Procedures*, v2.0;
7. NESDIS *Federal Information Security Management Act (FISMA) Inventory Management Policy and Procedures*, v2.0;
8. NESDIS *IT Security Training Policy and Procedures*, v2.1;
9. NESDIS *Continuous Monitoring Planning Policy and Procedures*, v2.1; and the
10. *Practices for Securing Open-source Project for a Network Data Access Protocol Server Software in NESDIS Information Systems*, v3.1.

These publications are part of the NESDIS-wide effort to maintain and enhance its foundation of NESDIS IT security policies and implementation practices that align with the latest Department of Commerce and NOAA policies, requirements, and standards. I wish to thank all who contributed reviewing and commenting on the drafts prior to publication to ensure that they are complete, current,

NESDIS Quality Procedure [NQP] – 3405
Revision 2.2

Effective Date: September 28, 2012
Expiration Date: Until Superseded

and meaningful. These documents will be posted to the Chief Information Division's Web site at https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/itsecurityhandbook.php. If you have any questions, please contact the NESDIS IT Security Officer, Nancy DeFrancesco, at Nancy.DeFrancesco@noaa.gov or phone (301) 713-1312.

NESDIS IT SECURITY TRAINING POLICY AND PROCEDURES

Record of Changes/Revisions

Version	Date	Section	Author	Change Description
Draft 1.0	7/24/2009	All	Noblis	Initial Draft
Draft 1.1	8/19/2009	All	ITSO	Updated for ISSO comments
Pre-final draft 1.2	9/15/2009	All	ITSO	Updated for final comments and finalize for CIO signature.
Final v1.0	9/30/2009	Date	ITSO	Finalize
Draft v2.0	2/23/2012	All	A.Kuhn	Update
Final v2.1	09/28/2012	Version number and date	N. DeFrancesco	Accept all changes and finalize for CIO approval.

1.0 Background and Purpose

Federal Information Security Management Act ([FISMA], Public Law 107-347) requires training of personnel in information technology (IT) security concepts, and the Code of Federal Regulations (5 C.F.R 930.301) requires that agencies “provide role-specific training in accordance with the National Institute of Standards and Technology (NIST).” NIST identifies a series of baseline security controls in Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, related to security awareness and training (AT). NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, and 800-16, *Information Technology Security Training Requirements*, provide guidance on developing an IT security training program. These NIST guides support the requirements specified in FISMA and the Office of Management and Budget Circular A-130, Appendix III. The Department of Commerce (DOC) *Information Technology Security Program Policy* (ITSPP) and the National Oceanic and Atmospheric Administration (NOAA) *IT Security Manual* mandate IT security training requirements.

Security training is integral to the safeguarding of National Environmental Satellite, Data, and Information Service (NESDIS) information systems. It facilitates the ability of NESDIS personnel to function effectively in their assigned roles, thus mitigating risk.

The purpose of this document is to communicate the NESDIS-specific policy and document the implementation procedures for compliance with the DOC ITSPP and NOAA *IT Security Manual* requirements.

2.0 Scope

NIST 800-16 delineates between three levels of learning – awareness, training, and education – with awareness identified as the pre-requisite to training. This document focuses on security training. Neither security awareness nor education will be addressed in this document. This is because NOAA provides and manages security awareness training (control AT-2) for the entire organization as a Common Control. Identification of formal education requirements is an aim of the hiring process; however, this does not preclude use of this document as guidance to determine hiring requirements or personnel qualifications.

3.1 Roles, Responsibilities, and Coordination

“The DOC ITSPP (Section 3.0) defines as significant information security roles, the following: DOC and OU [Operating Unit] CIOs, AOs [Authorizing Officials], Information SOs, IOs [Information Owners], DOC and OU CISOs/SAISOs/ITSOs, ISSOs, CAs [Certification Agents], IT Security Incident Response personnel and key contingency roles.” Within NESDIS, role-appropriate training (referred to herein as “role-based training”) is required for the following significant IT Security roles, at a minimum:

3.2 Chief Information Officer (CIO)

The NOAA Assistant CIO for Satellite and Information Services is responsible for ensuring that they, and all personnel under their purview who are assigned to a significant IT security role (mainly the IT Security Officer), complete role-based training within 60 days of appointment and annually thereafter. CIOs must notify these personnel of their significant IT Security role within 10 days of appointment.

3.3 Authorizing Official (AO), co-AOs, and AO Designated Representatives (AODRs)

The AO is responsible for ensuring that they, and all personnel under their purview who are assigned to a significant IT security role (mostly System Owners and Information Owners), complete role-based training within 60 days of appointment and annually thereafter. AOs must notify these personnel of their significant IT Security role within 10 days of appointment. The AO is responsible for maintaining records of training completion for these personnel and informing the NESDIS ITSO regarding training progress on a monthly basis.

3.4 System Owner (SO)

The SO is responsible for ensuring that they, and all personnel under their purview who are assigned to a significant IT security role (Information System Security Officers, system/network administrators, Information Owners, and contingency planning personnel), complete role-based training within 60 days of appointment and annually thereafter. SOs must notify these personnel of their significant IT Security role within 10 days of appointment. The SO is responsible for maintaining records of training completion for these personnel and informing the NESDIS ITSO regarding training progress on a monthly basis. The SO also determines and obtains necessary funding for ensuring resources are available to provide training. SOs shall determine the level or extent of such security training required to support the security posture and delineate which training shall be mandatory to grant access to their systems.

3.5 Information Technology Security Officer (ITSO) including Alternate ITSOs and direct support staff

The ITSO is responsible for ensuring that they, and all personnel under their purview who are assigned to a significant IT security role, complete role-based training within 60 days of appointment and annually thereafter. ITSOs must notify these personnel of their significant IT Security role within 10 days of appointment. The ITSO is responsible for maintaining a central repository of personnel assigned to significant IT security roles and training completion for these personnel. The ITSO informs the NESDIS Assistant Administrator (AA) and Office Directors regarding training progress on a monthly basis in the NESDIS AA Monthly Staff Meeting performance metrics briefing.

3.6 Information System Security Officer (ISSO) Including Alternate ISSOs and Direct Support Staff

The ISSO is responsible for ensuring that they complete role-based training within 60 days of appointment and annually thereafter. The ISSO also supports the SO with identifying personnel in significant IT security roles, and in determining training needs and requirements. The ISSO assists the SO, as needed, with tracking, record retention, and monthly reporting to the ITSO. In this regard, ISSOs enforce mandatory training by requiring its completion prior to granting system access and shall require periodic refresher training for continued access.

3.7 Certification Agent (CA)

Within NESDIS, the ITSO serves as the CA for moderate- and high-impact systems (see section 3.4 for responsibilities). For low-impact systems, the CA is responsible for ensuring that they complete role-based training within 60 days of appointment and annually thereafter.

3.8 Information Owners (IO)

NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, defines the IO role as: “The information owner is an agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. The IO is responsible for establishing the rules for appropriate use and protection of the subject information (e.g., rules of behavior) and retains that responsibility even when the information is shared with other organizations. The owner of the information stored within, processed by, or transmitted by an information system may or may not be the same as the system owner. Also, a single information system may utilize information from multiple information owners. IOs should provide input to system owners regarding the security requirements and security controls for the information systems where the information resides.” The IO may also fill the SO or the system AO role. The IO is responsible for ensuring that they complete role-based training within 60 days of appointment and annually thereafter.

3.9 Key Contingency Roles

Within NESDIS, personnel who deploy as part of your Contingency Plan Testing Exercise are responsible for ensuring that they complete role-based training within 60 days of appointment and annually thereafter. New appointments may complete any of the risk management training courses made available on the NESDIS intranet at https://intranet.nesdis.noaa.gov/ocio/it_security/training/it_security_training.php#ISSO. Contingency training is a required element of the annual contingency planning exercise (whether table top or full deployment). Personnel who participate in the annual exercise satisfy their annual contingency training as part of the exercise.

3.10 Other Significant IT Security Roles as Defined by the SO

ITSPP section 4.2.2/Row 3 states that “Since there are numerous management, technical, and operational roles that include elements of information security, each OU is encouraged to define such roles based on need and/or specific areas that require skill enhancement.” Within NESDIS, these “additional roles” may include, but are not limited to: supervisors; account, application, database, network and system administrators; developers and programmers; and users. NESDIS SOs must identify these personnel/roles and document them in the System Security Plan (SSP) under the AT-3 control section if they elect to levy this requirement on the role within the confines of their system environment. Contact the ITSO for assistance in determining whether or not to identify an Administrator or Developer/Programmer as someone who should be identified as having a significant IT security role. Those who are identified should complete role-based training within 60 days of appointment and annually thereafter.

4.0 Management Commitment

The NESDIS Chief Information Division (CID) supports the NESDIS AA’s strong emphasis on training NESDIS personnel with significant IT security roles. Through the issuance of this policy and procedures, the CID demonstrates its commitment to establishing a foundation for mitigating risk through role-based IT security training.

5.1 Compliance

The NESDIS ITSO monitors – through periodic reviews and monthly performance metrics – documentation of training for personnel with significant IT security within NESDIS to ensure compliance with applicable laws, directives, policies, and guidance. The ITSO reports to the AA monthly, and to the CIO and Office Directors as necessary regarding compliance. The AA, CIO, and/or Office Directors may initiate actions as necessary to correct reported deficiencies, including reallocation of resources to improve implementation of security practices, or removal of an individual from their role as AO, SO, ITSO, or ISSO. Furthermore, in accordance with DOC ITSPP 4.2.2 Row 4, “if a user refuses to engage in, or cannot meet the training requirement due to extenuating circumstances, access to information and resources must be suspended or terminated, performance in an IT security role re-evaluated, and a risk-based decision made by the OU AO. This may result in administrative action, including discipline up to and including removal action.”

5.2 References

- DOC ITSPP section 4.2 (January 2009)
- NOAA *IT Security Manual* 212-1302, Appendix D (March 2008)

- DOC Commerce Interim Technical Requirements CTR 006: *Information System Security Training for Significant Roles, Version 5.0* (September 2010)

6.1 Policy

NESDIS-specific requirements for training of NESDIS personnel assigned to significant IT security roles (as listed in section 3.0) shall align with the requirements of DOC ITSP section 4.2.2 (control AT-3) and provide for the maintenance of training records in accordance with DOC ITSP section 4.2.4 (control AT-4). By the end of each fiscal year, all (100%) of NESDIS personnel with significant IT security responsibilities must have completed the corresponding number of minimum training hours for the role in which they are assigned (see section 7.2.1).

6.2 Policy Maintenance

The NESDIS ITSO shall review this policy and procedures bi-annually and update as necessary to reflect implementation challenges and new requirements. All updates to this policy shall be subject to a NESDIS-wide vetting process providing an opportunity for stakeholders to comment on the programmatic implications of updates.

6.3 Policy Feedback Process

NESDIS personnel are encouraged to notify the ITSO via e-mail at nesdis.it.security@noaa.gov regarding any errors found in the document or other clarifications or updates that are required.

6.4 Policy Effective Date

This policy is effective within 30 days of issuance.

7.1 Procedures for NESDIS Personnel with Significant IT Security Roles

Role-based training prepares and enables an individual to function effectively in their appointed role. The NESDIS IT Security Training Program for personnel with significant IT security roles includes Baseline Training and Annual Refresher Training appropriate for each role. The NESDIS ITSO must ensure that training resources are available to personnel and that personnel complete training consistent with NOAA and DOC requirements.

7.2 Baseline IT Security Training Procedures

The Baseline IT Security training includes those training materials available on the NESDIS CID intranet at https://intranet.nesdis.noaa.gov/ocio/it_security/training/it_security_training.php and includes review of the laws, regulations, and guidance referenced therein that are

foundational to the NESDIS IT Security Program. Within 60 days of assignment, personnel with a significant IT security role shall complete the online training appropriate for their role (i.e., IT Security Training for NESDIS AOs, IT Security Training for NESDIS SOs, or NESDIS IT Security Training for NESDIS ISSOs) and complete the attestation of reviewed laws, regulations, and guidance following the below procedures.

7.2.1 Online NESDIS Training

The procedures below provide the steps for completing online training available through the NESDIS CID Intranet.

- Step 1.** Go to the following location on the NESDIS CID intranet:
https://intranet.nesdis.noaa.gov/ocio/it_security/training/it_security_training.php
- Step 2.** Select the training module appropriate for your role (modules are organized by role such as AO, SO and ISSO). Although training materials are identified by role, NESDIS personnel are encouraged to review any materials of interest.
- Step 3.** Open or save the file to your local system and begin reviewing the material.
- Step 4.** Notify the NESDIS ITSO upon completion of the course by sending an email to the NESDIS IT Security Team at nesdis.it.security@noaa.gov.
- Step 5.** The NESDIS IT Security Team will send a certificate of completion within five business days and record completion in the NESDIS CID central records database.

7.2.2 Laws, Regulations, and Guidance

Review applicable laws, regulations, and guidance for their role as identified in Appendix A and notify the NESDIS CID attesting to completion using the Appendix A template. Upon completion of the document review, system personnel must notify the SO in writing attesting that they have completed the required review (see template in Attachment A). A copy of the training record must be submitted to the NESDIS ITSO.

SOs may add to the list of laws, regulations, and guidance listed in Attachment A. SOs should consult the ISSO and ITSO to identify other relevant standards and guidance in addition to the defined Basic Training to

include in the training plan. SOs can accomplish this by first linking roles and responsibilities of individuals to specific controls in NIST 800-53.

Using this link, SOs can use Appendix H of NIST Special Publication 800-53; *Standards And Guidance Mappings: Crosswalk Between NIST Standards and Guidelines and Security Controls* to determine what standards and guidance should be reviewed by system personnel. Another approach for identifying standards and guidance for review is to consider specific system characteristics and have those involved in the design, development, implementation, and/or management of those technologies review NIST's listing of publications by Topic Cluster (<http://www.csrc.nist.gov/publications/PubsTC.html>). The U.S. Computer Emergency Readiness Team (US-CERT) reading room at http://www.us-cert.gov/reading_room/ also provides role-based instructional publications.

7.3 Role-Based Annual Refresher Training

Information on training resources is available through the NESDIS IT Security Program at

https://intranet.nesdis.noaa.gov/ocio/it_security/training/it_security_training_index.p hp. Training materials and resources include:

- Links to no-cost role-based NESDIS-specific training presentations on roles and responsibilities and the NESDIS Assessment and Authorization (A&A) Process
- NIST training video and presentation on risk management
- Links to External Training and Professional Certification Resources, including:
 - [Information Systems Audit and Control Association \(ISACA\)](#)
 - [International Information Systems Security Certification Consortium \(ISC\)²](#)
 - [System-Administration, Audit, Network, and Security \(SANS\) Institute](#)

In addition to furnishing these training resources online through the NESDIS CID intranet, the NESDIS CID will provide information via email and during the monthly Information Resource Management Team (IRMT) IT Security Team meetings regarding new or existing training opportunities. NESDIS personnel are encouraged to use these monthly meetings to share experiences, provide suggestions, and discuss opportunities related to security training. For more information on IRMT IT Security Team meetings and off-site workshops, please contact the NESDIS IT Security Team via email at nesdis.it.security@noaa.gov.

NOAA provides training resources on its website at <https://www.csp.noaa.gov/tea>. In addition, Appendix D of the *IT Security Manual*, March 31, 2008, identifies mandatory IT security training requirements for SOs, ISSOs, Network Administrators, and System Administrators (see Table 19: Mandatory IT Security Awareness, Training, and Education Requirements).

The SO, in coordination with the ISSO, may create a training program plan to address requirements for these and other personnel with significant IT security responsibilities during various stages of the system development life cycle. NOAA provides a template for a *Security Education, Training, and Awareness Program Plan* that may facilitate managing a system-specific role-based training program for system personnel (template will be posted to the NESDIS IT Security Handbook website at https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/it_security_handbook.php).

7.3.1 Role Identification and Required Minimum Training Hours

The following table lists roles that have a significant IT security responsibility and the corresponding number of minimum training hours required to complete per fiscal year:

Table 1 Role Identification and Required Minimum Training Hours

<u>Significant Role</u>	<u>Minimum Annual Requirement</u>
Information Technology Security Officer (ITSO)	Professional Certification (20 hours)
Certification Agent/Security Controls Assessor/Certifier	Professional Certification (20 hours)
Authorizing Official (AO)	1 hour
System Owner (SO)	2 hours
Information System Security Officer (ISSO)	Professional Certification (20 hours)
Information Owner (IO)	1 hour
Key Contingency Personnel	4 hours
Database Administrators and Systems Administrators, ISSO support personnel	3 hours

7.4 Role-Based Professional Certifications

As required by DOC CITER-006, ISSOs are required to obtain and maintain professional certification. Therefore, the hours are dictated by the certifying organization's annual renewal requirements for the professional certification held. For non-certified ISSOs, certification exam preparation training would satisfy the requirement as long as it is completed by the end of the fiscal year. Alternately, ISSOs may complete training through other sources as recommended by the NESDIS ITSO or as posted on the NESDIS IT Security Training website at https://intranet.nesdis.noaa.gov/ocio/it_security/training/it_security_training_index.php. Please submit PDF copies of completion certificates or the official Continuing Professional Education (CPE) transcript from the certifying organization that reflect sufficient hours to cover at least the minimum annual hours required for the maintenance of your specific credential to nesdis.it.security@noaa.gov. Table 2 Recommended Certifications by Significant IT Role, identifies certification options appropriate for each role.

Table 2 Recommended Certifications by Significant IT Role

Certification	Target Role/Audience
CAP	CIO, AO, AODR, ITSO, SO, CA
CISA	Security Controls Assessors (SCAs) Systems audit, control, and security professionals
CISM	ITSOs, ISSOs, SOs and those who manage, design, oversee and/or assess information security programs
CISSP (or Associate)	ISSOs and ITSOs with at least five years experience although “CISSP Associate” certification can be obtained with less than five years experience
CISSP-ISSMP	ISSOs and ITSOs with at least 2 years experience in management
GISF	AOs, CIOs, IOs, SOs
GSE	For ITSOs, ISSOs, and System Administrators who already have three GIAC certifications (GSEC, GCIA, and GCIH) with hands-on experience in each. Advanced knowledge in the following domains is also required: intrusion detection systems and Traffic Analysis, Incident Handling, IT Security, Security Technologies, and Soft Skills.
GSEC	ITSOs, ISSOs, System Administrators
GSLC	CIOs, ITSOs, SOs
SCNA	Network Administrators who already have an SCNP certification.
SCNP	Network Administrators
Security+	ITSOs, ISSOs, or Administrators with experience in system security, network infrastructure, cryptography, assessments and audits
SSCP	Individuals working towards security role related to network security, security analysis, or security administration. Appropriate for those where security is not a primary role, such as System, Network, or Database Administrators.
GSNA	SCAs
CSIH	Individuals responsible for incident handling/incident response with three years of experience in incident handling or security-related experience.
GCIH	Individuals responsible for incident handling/incident response

Certification	Target Role/Audience
CISSP-ISSAP	Chief Security Architects and Analysts with 2 years experience in system architecture.
CISSP-ISSEP	Security engineering professional who must incorporate security into projects, applications, business processes, and all information systems.
GCIA	Individuals responsible for network and host monitoring, traffic analysis, and intrusion detection

8.1 IT Security Training Program Management Procedures for SOs and the ITSO

8.2 Identify Personnel in Significant IT Security Roles

The SO shall list in the SSP, in the AT-3 control section, all roles associated with the system that are identified as significant under section 3.0 of this document, as well as any additional roles as deemed appropriate by the SO in consultation with the ISSO and ITSO (see section 3.9).

Ensure that new appointments are notified of their significant role within 10 days of appointment. This can be accomplished through the Performance Plan elements and activities for federal personnel, and by written memo to contractor personnel (through the COR).

The SO will notify the ITSO of new IT Security role appointments within 10 business days of appointment, and will incorporate the role notification into the employee orientation package in-processing procedures. The notification will be sent via email to the nesdis.it.security@noaa.gov and will include a copy of the new role appointment memo. Sample appointment memos for SOs and ISSOs will be posted to the NESDIS IT security intranet site at https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/it_security_handbook.php.

In accordance with DOC policy, individuals with significant IT Security responsibilities must complete at least role-based training course within the first 60 calendar days from role appointment notification. NESDIS provides resources for role-appropriate training on the intranet at https://intranet.nesdis.noaa.gov/ocio/it_security/training/it_security_training_index.php.

8.3 Reporting and Tracking

Quarterly, or more frequently as needed, the ITSO will distribute draft training status reports to the Office Directors and SOs. SOs must provide the ITSO with any updates to the training data. The SO or ISSO shall provide updated training data via email to nesdis.it.security@noaa.gov. The ITSO shall report monthly to the NESDIS AA on the status of training completed by personnel with significant IT security roles as part of the NESDIS CID Monthly status report, and report to NOAA and DOC as requested for FISMA reporting.

8.4 Record Retention

The NESDIS CID will maintain training records for a period of three years.

APPENDIX A: LAWS, REGULATIONS, AND GUIDANCE REVIEWED TEMPLATE

Complete the identification information and check all publications reviewed. Sign and date where indicated and send a PDF format file to nesdis.it.security@noaa.gov

Name: _____ **System ID:** _____

IT Security Role(s) (see section 3.0 of the *NESDIS IT Security Training Policy and Procedures*. List all that apply if you fill multiple roles): _____

Law/ Regulation/ and/or Guidance (note: all NIST and FIPS publications are available online at http://www.csrc.nist.gov/)	Required Reading per Role is marked with an “X”				Check if completed
	CIO AOs AODRs	SOs IOs CAs	ITSO and ISSO	Other key personnel	
NOAA IT Security Manual 212-1300 (includes sections 1301, 1302, and 1305) (https://www.csp.noaa.gov/policies)		X	X		
OMB Circular A-130, Appendix III Security of Federal Automated Information Resources (http://www.whitehouse.gov/omb/circulars/a130/appendix_iii.pdf)	X	X	X		
FIPS Publication 199, Standards for Security Categorization of Federal Information and Information System	X	X	X		
FIPS Publication 200, Minimum Security Requirements for Federal Information and Federal Information Systems	X	X	X		
NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems	X	X	X	X	
NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems	X	X	X	X	
NIST Special Publication 800-39, (second public draft) NIST Risk Management Framework	X	X	X		
NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems	X	X	X	X	
NIST Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems			X	X	

Law/ Regulation/ and/or Guidance (note: all NIST and FIPS publications are available online at http://www.csrc.nist.gov/)	Required Reading per Role is marked with an “X”				Check if completed
	CIO AOs AODRs	SOs IOs CAs	ITSO and ISSO	Other key personnel	
NIST Special Publication 800-59, <i>Guide for Identifying an Information System as a National Security System</i>		X	X		
NIST Special Publication 800-60, <i>Guide for Mapping Types of Information and Information Systems to Security Categories</i>		X	X		
NIST SP800-18 revision 1, <i>Guide for Developing Security Plans for Federal Information Systems</i>		X			
Procurement Memorandum 2006-06: <i>Information Security in Acquisitions</i> , http://oamweb.osec.doc.gov/docs/PM-2006-06-InformationSecurity-in-Acquisitions.pdf		X	X		
NOAA IT Security Configuration Guides: https://www.csp.noaa.gov/noaa/ncirt/configurations.html			X		
Web Banner Guidance: https://www.csp.noaa.gov/banners/			X		
DOC Remote Access Policy: https://www.csp.noaa.gov/policies/docs/DOC_Remote_Access_Policy_Dec02.pdf		X	X		
DOC IT Security Program Policy, CITRs and ITSPP Appendices (http://home.commerce.gov/CIO/ITSITnew/IT_Security_Program_Documentation.html)		X	X		
NIST Special Publication 800-100, <i>Information Security Handbook: A Guide for Managers</i>	X	X			
NIST Special Publication 800-47, <i>Security Guide for Interconnecting Information Technology Systems</i>			X		
NIST Special Publication 800-34, <i>Contingency Planning Guide for Information Technology Systems</i>			X		
NIST Special Publication 800-40 Version 2.0, <i>Creating a Patch and Vulnerability Management Program</i>		X	X		
DOC and NOAA policy for Wi-Fi networks		X	X		

By my signature below, I attest that I have reviewed the indicated publications as required by the NESDIS IT Security training program Basic IT Security Training requirements.

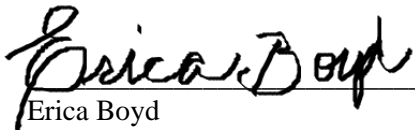
Signature

Date

Approval Page


Document Number: NQP-3405, Revision 2.2	
Document Title Block: IT Security Training Policy and Procedures	
Process Owner: NESDIS Chief Information Division	Document Release Date: September 28, 2012

Prepared by:


Erica Boyd
Ambit- Associate Consultant
NESDIS Chief Information Office

3/26/15
Date:

Approved by:


Irene Parker
Assistant Chief Information Officer - Satellites

3/26/15
Date:

Document Change Record

VERSION	DATE	CCR #	SECTIONS AFFECTED	DESCRIPTION
2.2	March 26, 2015	----	ALL	Baseline NQP-3405