

2171

REGISTRO DE CONTRATOS  
TOMO 17 PAGINA 21  
CONTRATO NUM. 2008-000 119

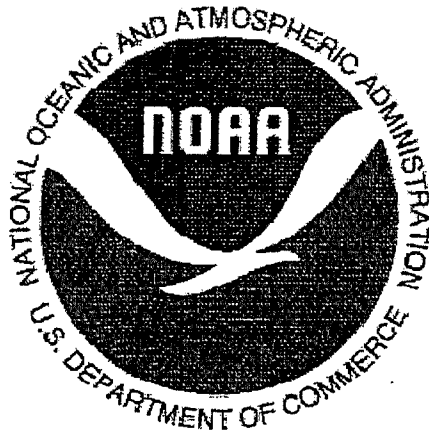
# INTERCONNECTION SECURITY AGREEMENT

Between National Oceanic and Atmospheric Administration  
(NOAA)  
The National Weather Service (NWS)

And  
University of Puerto Rico in Mayaguez  
Puerto Rican Seismic Network (PRSN)

20 AUG 20 AM 11:05

OFFICE ASSISTANT LEGAL  
RUMI



July 17, 2007

NOAA NWS CIO1 1325 East-West Highway, Room 5800 Silver Spring, MD 20910	
---	--

## Revision History

Version	Date	Author/Modifier	Change Description
0.1	7/20/2007	Sam Musa	Initial version

Notify the document author for corrections or change requests.

---

## SECTION 1 - INTERCONNECTION STATEMENT OF REQUIREMENTS

NOAA's National Weather Service, an agency of the Department of Commerce, and Puerto Rican Seismic Network have an operational requirement for an interconnection between the NOAAnet Wide Area Network (WAN) operated by NWS and the Puerto Rican Seismic Network (PRSN) operated by the University of Puerto Rico in Mayaguez. Specifically, the purpose of the connection between the two systems is to support the exchange of seismic data in support of NOAA's Tsunami Warning Centers via the portion of the Sprint provided private IP Network known as NOAANet.

NWS provides weather, hydrologic, and climate forecasts and warnings for the United States, its territories, adjacent waters and ocean areas, for the protection of life and property and the enhancement of the national economy. The NWS also is responsible for providing Tsunami warnings, watches and information statements for the United States and its territories. The PRSN collects, analyzes and disseminates data and information to determine rapidly the location and size of all destructive earthquakes worldwide.

## **SECTION 2 - SYSTEM SECURITY CONSIDERATIONS**

This section summarizes the system security features and considerations for the NWS – PRSN interconnection. Further details are presented in the NOAAnet Security Plan, NOAA8204 which is attached to this interconnection agreement.

### **A. General Information/Data Description**

The PRSN transmits and receives seismic data as part of this interconnection. The transmitted data is unclassified and unencrypted.

### **B. Services Offered**

---

#### **Network Transport**

NOAA provides network transport services via an interconnection to the NOAA Wide Area Network (WAN), NOAAnet, established at a NOAAnet Customer Edge (CE) router located at the University of Puerto Rico in Mayaguez. NOAAnet provides transport services over a carrier provided MPLS network which establishes Virtual Private Networks (VPNs) in support of specific communications requirements among customers. The PRSN interconnection will transit the Tsunami VPN exclusively.

The NWS operates NOAAnet following NIST security guidelines for Certification and Accreditation (C&A). The NOAAnet C&A is documented as NOAA8204 and has been granted Authority to Operate (ATO) by the National Weather Service Assistant Administrator in July 2007.

### **C. Data Sensitivity**

The data to be transmitted by the PRSN is considered to have a Low confidentiality categorization. The classification level of the information to be exchanged is unclassified.

### **D. User Community**

The user community served by the interconnected system includes the NWS Tsunami Warning Centers (TWCs) and the PRSN. PRSN provides seismic data and the TWCs exchange Tsunami information with PRSN. The user community is strictly limited to those organizations that have access to the NOAAnet Tsunami VPN.

### **E. Information Exchange Security**

- No data is exchanged between the interconnected systems.

- All NOAA system boundaries are monitored and protected by stateful firewalls. NOAA does not encrypt customer data traversing the network, however all access, either network based or via out of band (dial up) access to NOAA edge devices requires two factor authentication and is encrypted in accordance with FIPS140-2.

#### **F. Trusted Behavior Expectations**

The following section outlines expectations regarding Rules of Behavior to be followed by the NWS and the PRSN to protect information exposed to this interconnection. NWS reserves the right to terminate this agreement if the other party fails to comply with these expectations.

- NOAA employees and contractors agree to conform to the guidelines in accordance with Appendix A NOAA Rules of Behavior. Appendix A is being provided for informational purposes only.
- NWS expects that PRSN will follow Incident Reporting procedures outlined in section H of this document.
- NWS expects that the PRSN will take appropriate measures to prevent operational attacks, such as denial of service.
- NWS expects that the PRSN will maintain access controls at all of its external network peering points in a manner that prevents third party network traffic from accessing the NWS network at the peering points.
- NWS will take appropriate measures to prevent operational attacks, such as denial of service attacks.
- NWS will maintain access controls at all of its external network peering points in a manner that prevents non-NWS network traffic from accessing the PRSN network at interconnection points.

#### **G. Formal Security Policy**

NWS is governed by the information security policies of the Federal Government, including OMB, Department of Commerce and NOAA as noted below:

- Privacy Act of 1974, Public Law 93-579
- Computer Security Act of 1987, Public Law 100-235
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources
- Computer Fraud & Abuse Act of 1986, as amended, Public Law 99-474
- Federal Information Security Management Act (FISMA)
- Information Technology Management Reform Act (Clinger-Cohen)

- The NOAA IT Security Manual as authorized by NOAA Administrative Order 212-13
- NOAA Administrative Order 212-14
- NOAA Administrative Order 216-100
- DOC IT Security Program Policy and Minimum Implementation Standards
- DOC Policy on Password Management
- DOC Policy and Implementation for Remote Access
- DOC IT Security Handbook
- DOC user Guide for Developing and Evaluating Security Plans for Unclassified Federal Automated Systems
- NOAA WWW Appropriate Use Policy
- NOAA Style and Content Guidelines for the World Wide Web

#### H. Incident Reporting

The PRSN is requested to report suspected security incidents to the NOAAnet NOC at 1-888-NOAANET (1-888-662-2638) in addition to their internal procedures. NOAA will report IT security incidents to the NOAA Computer Incident Response Team (NCIRT) at 301-713-9111.

The NOAAnet NOC will then follow the procedure outlines in accordance with the NWS Telecommunications Operations Center IT Security Response Procedure attached as Appendix B.

The PRSN Point of Contact in the case of a security incident is:

Name and/or Title:

Phone Number:

Secure Email

#### I. Audit Trail Responsibilities

NOAAnet edge devices are configured to log all sessions and all unsuccessful access attempts. Logs are compressed and archived on a monthly basis. Archives are maintained for one year. Logs include event type, date and time. NOAAnet clients are responsible for logging activity on their side of the NOAAnet boundary.

NWS does not require audit information from the PRSN, and will not access audit information across the interconnection.

#### J. Security Parameters

Access across NOAAnet is permitted based on both source and destination IP

address and protocol.

**K. Operational Security Mode**

NWS supports the following "Protection Levels" and "Levels-of-Concern for Confidentiality, Integrity, and Availability" for data transmitted across this interconnection:

- Confidentiality – Low
- Integrity – Moderate
- Availability – High

---

~~Protection Levels and Levels-of-Concern for Confidentiality, Integrity, and Availability supported by PRSN are as follows:~~

- ~~• Confidentiality –~~
- ~~• Integrity –~~
- ~~• Availability –~~

**L. Training and Awareness**

Not required.

**M. Specific Equipment Restrictions**

Customers and partners connecting to the NWS NOAA net wide area network shall use equipment that is in compliance and has been approved by their network carrier and NWS for network interconnection.

**N. Dial-Up Connectivity**

Customer dial up connectivity is not permitted. Dial up connectivity for the purpose of out of band access to NOAA net customer edge routers is permitted only to NOAA net engineers using encrypted modems and two-factor authentication.

**O. Security Documentation**

The NWS and NOAA net operate in accordance with System Security Plans that satisfies the requirements outlined in NIST Special Publication 800-53.

SECTION 3 - TOPOLOGICAL DRAWING

NOAAnet Access Design, Layer 2  
Small/Medium: CE to Customer

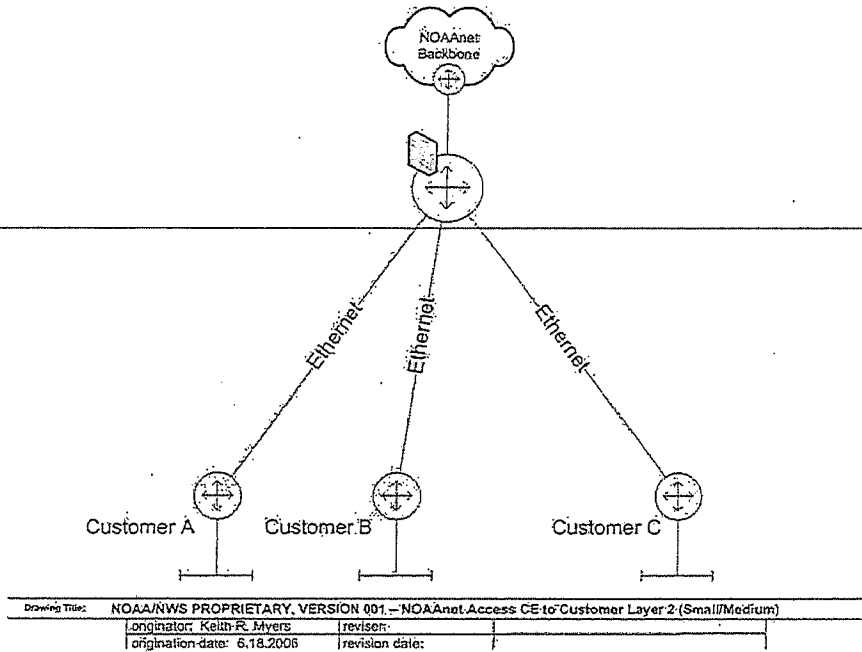



Figure1. Generic NWS and PRSN interconnection diagram



**SECTION 4 - SIGNATORY AUTHORITY**

This ISA is valid for one year after the last date on either signature below. At that time it will be reviewed, updated if necessary, and revalidated. This agreement may be terminated upon 30 days advanced notice by either party or in the event of a security exception that would necessitate an immediate response.

National Weather Service Designated Accrediting Authority	PRSN Designated Accrediting Authority
<p>(Signature Date)</p>	 <p>(Signature Date)</p> <p>12 Sept 2007</p>

L

NOAA's National Weather Service  
Office of the Chief Information Officer  
Telecommunication Operations Center

**Appendix A**

Document: NOAA Rules of Behavior

---

2.

## Overview

NOAA provides access to computing resources (hardware, software, and data) to its employees and contractor staff. These resources are provided to facilitate completion of assigned responsibilities, with prior authorization. The policies and procedures governing use of NOAA computing resources are detailed in NOAA Management Directives. Individuals who are authorized to use NOAA computing resources must comply with NOAA Management Directives and the specific Rules of Behavior listed below.

## Roles Assignments

### End User Responsibilities

---

- Users are required to report known or suspected incidents, including unauthorized use of NOAA computer resources; lost, missing or stolen IT hardware (laptop computers, Personal Digital Assistants, removable memory devices); and loss of any potential Personally Identifiable Information (PII), to their local ITSSO, and to the NOAA Computer Incident Response Team (N-CIRT), by calling (301) 713-9111 and using NOAA Form 47-43. All incidents must be reported with 24 hours of detection. Incidents involving potential release of PII must be reported to the N-CIRT within one hour of detection.
- Use NOAA computers only for lawful and authorized purposes.
- Comply with safeguards, policies, and procedures to prevent unauthorized access to NOAA computer systems.
- **Passwords.** User passwords are required to comply with the DOC IT Security Program Policy and Minimum Implementation Standards Policy for Password Management (Appendix G). Users passwords must be changed at least every 90 days and at a minimum contain at least 8 characters consisting of numbers, letters and special characters. Passwords cannot be reused for 2 years and can't contain dictionary words (spelled forward and backwards.) Do not write down or share your logon or account password with anyone (including the Help Desk). Users must log-off or use a password-protected screen saver whenever leaving their workstation unattended.
- **Individual Accountability.** NOAA computer users are accountable for their assigned User IDs, passwords, and IT equipment. Each user must have a unique ID to access NOAA systems. User IDs are used to identify an individual's actions on NOAA systems and the Internet. Individual user activity is recorded, including sites and files accessed on the Internet. Individual employees must safeguard IT equipment, including laptop computers, Pads, and removable storage devices (including "thumb drives") assigned to them. **Employees can be held individually financially responsible for missing, lost, stolen, or damaged property if it is determined to be the result of employee negligence**

- **E-mail.** Chain letters, games, union announcements and threatening, obscene, or harassing messages are not allowed. Management must approve use of broadcast features. Do not open unsolicited or suspicious e-mail messages or their attachments, do not forward chain mail, and do not generate or send offensive or inappropriate e-mail messages, images, or sound files. Limit distribution of e-mail to only those who need to receive it.
- **Anti-Virus Protection.** Users are required to use regular updated anti-virus software while using or accessing government IT systems and resources. When your workstation begins an update of its anti-virus software, let that update finish. Use authorized virus scanning software on your workstation or PC and your home computer. ~~Know the source before using diskettes or downloading files. Scan files~~ for viruses before execution. Minimize the threat of viruses: (1) Write-protect diskettes and CD's, (2) Virus check any foreign data source, and (3) Never circumvent the anti-virus safeguards on the system.
- **Data Backups.** Ensure that data are backed up, tested, and stored safely.
- **Protection of ITS Hardware.** Users are responsible for safeguarding IT hardware assigned to them from loss and damage. Users must know the reporting requirements for lost, stolen, or damaged hardware.
- **Protection of copyright licenses (software).** Users using government-owned equipment are not permitted to download and/or install any software application(s) on systems without prior System Owner approval. All software must be properly licenses prior to installation on any government-owned equipment. Audit logs will be reviewed to determine whether employees attempt to access government-owned systems or IT resources on which valuable, commercial-off-the-shelf or government software resides, but to which users have not been granted access.
- **Copyrighted Software.** Unauthorized copying of copyrighted software is prohibited. Users are required to comply with the DOC Copyrighted Software Policy and Title 17, United States Code, Section 106.
- **Connections to the Internet.** All desktop Pac's, workstations and servers that have access to the Internet and its use must be in accordance with the DOC and NOAA Internet Use Policies.
- **Use of Government Equipment.** Users are permitted limited personal use of government-owned equipment during non-duty hours (before scheduled work hours, lunch times, and after work hours). Personal use of government-owned equipment and IT resources must not incur any additional costs to the government and/or violate any federal regulations, DOC or NOAA policies. Activities specifically not permitted on government-owned IT resources include, but are not limited to the following: a) private commercial business activities or profit making ventures; b) engagement in matters directed toward the success or failure of a political party, c) engagement in any prohibited direct or indirect lobbying; d) use that could generate or result in an additional charge or expense to the Government; e) viewing, obtaining, creation, distribution, or storing of sexually explicit material; f) participation in or encouragement of illegal activities or the

intentional creation, downloading, viewing, storage, copying, or transmission of materials that are illegal or discriminatory; g) Use of Government e-mail addresses in a manner that will give the false impression that an employee's otherwise personal communication is authorized by the Department; h) engagement in unauthorized charitable fund raising (see the Broadcast E-Mail Policy) or soliciting volunteers to raise funds; and/or i) activity that would bring discredit on the Department or violation of any statute or regulation, including applicable copyright laws. Personally purchased software is not allowed on government equipment. DOC IT Security Program Policy and Minimum Implementation Standards Policy for Peer-to-Peer File Sharing (Appendix I) restricts the use of Peer to Peer file sharing. Users will not use Peer to Peer (P2P) connection sharing for transferring copyrighted files.

- **Remote Access.** Designated managers may authorize remote access to specific IT systems and resources of specific systems for remote user access. All remote users are required to review and comply with all aspects of the DOC and NOAA Remote Access Policy and sign the Remote Access Agreement. These rules of behavior apply for all remote accesses.
- **Data Destruction.** Properly dispose of unneeded data: (1) Do not throw sensitive hard copy into a wastebasket (shred or burn). (2) Delete sensitive information from memory on hard drive and diskettes permanently by overwriting. Ask ITSO for aid.
- **NOAA Security Awareness Training.** Users are required to complete the NOAA IT Security Awareness course annually.
- Users need permission from appropriate NOAA officials before they discuss security practices or anti-piracy practices with external organizations or individuals.

### Supervisor/Management Responsibilities

NOAA supervisors and management officials are responsible for ensuring an adequate level of protection is afforded to IT resources through an appropriate mix of managerial, operational, and technical controls.

In addition to the rules that apply to all end users, each supervisor/application system manager is responsible to ensure that:

- All employees/contractors belonging to or performing work within the supervisor's organization:
  - Have appropriate security clearances.
  - Behave in a manner consistent with the protection and security of information, data, software, hardware, and systems assigned to or used by them.

- Employee/contractor access privileges are granted to information and systems, being mindful that:
  - Users should not have access privileges (or software) other than for official business.
  - Access privileges must be removed as soon as the need expires or within 24 hours of separation from NOAA.
- All employees/contractors have current knowledge of these Rules of Behavior, including specialized rules for specific data sets and systems that govern the use of workstations, the network, databases, and other systems, and for instructing all who are assigned to or work within his/her organization regarding the existence and application of these rules.

---

### ~~Systems/Network/LAN Administrators Responsibilities~~

In addition to the rules that apply to all end users, each system/network/LAN administrator is responsible for:

- Supporting supervisors in their efforts to ensure employee compliance with DOC and NOAA Rules of Behavior. This includes specialized rules for specific information files and systems, for use of workstations, network privileges, databases, and other system features and functions, as well as legal requirements government use of proprietary software.
- Monitoring the security status of their systems, auditing activities, and reporting findings to the appropriate manager. The conduct of these activities has two basic components:
  - Routine/Regular:
    - Regular security monitoring (e.g., intruder detection).
    - Report violations.
    - Audit per NOAA standards and security plan.
  - Ad Hoc/Special efforts requested by management. Maintaining documented authorization from the appropriate supervisor(s) for granting or expanding access to system assets for NOAA employees, as well as for other individuals, organizations, or systems (For all items on the system/network/LAN that require controlled access control should be restricted according to group membership rather than individual permissions. This will provide easy accounting of who has access to what.)
- Dedicated account(s) for performing “root” or “super user” functions are to be used only when required.
  - Administrators should log in with the least amount of authority required to perform the task; i.e., not use “super user” status unless required.
  - Standard user account(s) for performing day-to-day activities that don’t require administrator authority are to be used.
- Obtaining authorization from (or adhering to a protocol established by) the appropriate supervisor(s) for the reconfiguration of equipment or software, and maintaining documentation of the changes and the authorization thereof. There must be management control over changes and reconfiguration that compromise

security. The administrator should operate within a standard range of previously agreed upon decision-making authority.

- The system/network/LAN administrator's responsibility is limited to those things that she/he could be reasonably expected to control. For example, changes to the CONFIG.SYS on a workstation attached to the LAN are not something for which the LAN administrator would be held liable either for authorization or for documentation. Corporate accounts may be established, with proper authorization, to be used by supervisors and managers to establish the requested access privileges for employees, in lieu of authorizing the LAN administrator to do so.

*Please indicate your acknowledgment:*

Accept     Deny

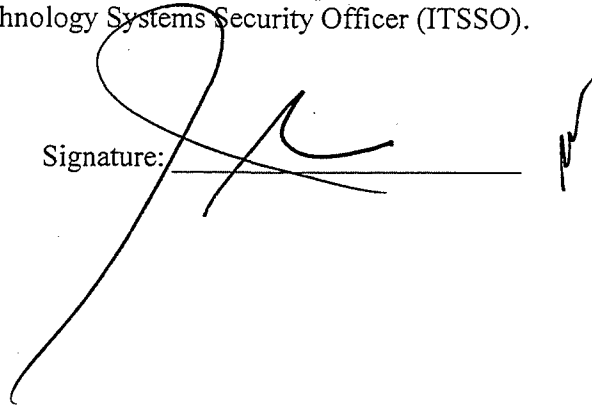
---

I understand, as an authorized user requiring access to NOAA automated information systems, that I am required to comply with NOAA regulations, policies, procedures, guidelines, and NOAA IT Systems Rules of Behavior regarding the protection of NOAA automated information systems from misuse, abuse, loss, or unauthorized access and understand the possible consequences of failing to comply. I will report security incidents or violations to my local Information Technology Systems Security Officer (ITSSO).

Date:

12-22-2007

Signature:



NOAA's National Weather Service  
Office of the Chief Information Officer  
Telecommunication Operations Center

Document Type: IT Security Policy & Procedure

## IT Security Incident Response Procedures

Effective Date: February 20, 2007  
Author: Larry Tun  
Reviewed and Approved by: Allan Darling/Sam Musa

Document Control Name: Incident Response Procedures.doc  
Version: 1.0  
Last update: July 13, 2007



## Revision History

Version	Date	Author/Modifier	Change Description
0.1	2/14/06	Larry Tun	Initial version
0.2	2/20/07	Sam Musa	Updated the initial version (added #1&5)
1.0	7/13/07	Sam Musa	Final draft

Notify the document author for corrections or change requests.

g

## Overview

This document outlines the tasks necessary to comply with NOAA Incident Response Policies. This document applies to all TOC employees and contractors.


TOC Management has reviewed and approved this procedure. Failure to comply with this procedure will result in appropriate management action. TOC staff must immediately report compliance failures to their team lead or branch manager.

Any issues that arise during the execution of this procedure that result in noncompliance with referenced policy should be immediately reported to the Information System Security Officer (ISSO).

## Roles Definitions

- I. The **Information Systems Security Officer (ISSO)** is responsible for managing all aspects of security within TOC operations. When alerted of an incident, the ISSO shall disseminate all information with the appropriate personnel.
- II. The **OCIO IT Security Officer (ITSO)** is responsible for managing all aspects of security within the NWS Program. The ITSO shall be informed and updated of all security incidents.
- III. The **NOAA Computer Incident Response Team (N-CIRT)** shall lead the efforts in investigating and resolving security incidents. Once all appropriate personnel are aware of the incident, system administrators shall collaborate directly with N-CIRT until the incident case is closed.

## Roles Assignments

- 
- I. **Information Systems Security Officer (ISSO):**  
Sam Musa, NWS Telecommunications Gateway ISSO
  - II. **OCIO IT Security Officer (ITSO):**  
Harry Tabak, NWS ITSO
  - III. **NOAA Computer Incident Response Team (N-CIRT):**  
Various members

## Procedure

When a TOC employee or contractor suspects that an IT security incident has occurred, s/he shall adhere to the following procedures in reporting and resolving the incident.

1. **DO NOT TALK TO THE NEWS MEDIA.** Whenever a government system has been compromised, there may be legal issues to be addressed. Thus, always contact NOAA General Counsel and your public affairs office before considering talking to the news media.
2. Prior to reporting an incident, without accessing the affected systems, TOC personnel shall gather as much of the following information as possible:
  - a. A description of the discovery.
  - b. Data and time of detected events.
  - c. Who was the source (if any)? [IP, Port, Protocol]
  - d. What TOC servers are affected/targeted?
  - e. What Operating Systems are affected servers running?
  - f. What is the estimated impact (e.g. disruptions, hardware loss, etc)?
3. TOC personnel shall then attempt to notify an emergency contact. The NWS Notification Card and TGWEB contain emergency contact phone numbers. TOC personnel shall attempt to phone the contacts in the following order until one of the emergency contacts is reached.
  - a. TOC ISSO
  - b. NOAA CIRT (N-CIRT, 301-713-9111)
  - c. OCIO ITSO
  - d. Appropriate TOC Branch Chief

NOTE: All suspected incidents are required to be reported within 1 hour of discovery.

4. The TOC personnel shall inform the emergency contact regarding all information relating to the incident.
5. The emergency contact shall then file a 47-43 Form with NOAA CIRT, with the TOC ISSO and appropriate Branch Chief included in all incident correspondence. A response with instructions can be expected within 24 hours from N-CIRT.

47-43 form can be accessed via the Internet. Please login to the form using your LDAP account. [https://www.csp.noaa.gov/V3\\_Form/index.php](https://www.csp.noaa.gov/V3_Form/index.php)

6. TOC personnel shall provide timely responses (< 24 hours) to all N-CIRT inquiries regarding the incident.

7. The System Administrators of the affected systems shall collaborate with the TOC ISSO and N-CIRT in investigating the incident, resolving all problems, and preventing further incidents. The process is completed when N-CIRT closes the incident report.

**Additional Information**

TOC adheres to the procedures and policies specified by the DOC Office of the CIO (see reference materials below). In the event that any portion of this document conflicts with DOC OCIO policies and procedures, OCIO policies and procedures will apply.

**Reference Materials**

This document and referenced documents and forms are available to all employees on the network drive in the directory

S:\CIO1\_D\IT Policies and Procedures\Security

Document description	File name or URL
DOC IT Security Program Policy	ITSPP 2005.pdf
47-43 Form	<a href="https://www.csp.noaa.gov/noaa/ncirt/itsecreport.html">https://www.csp.noaa.gov/noaa/ncirt/itsecreport.html</a>