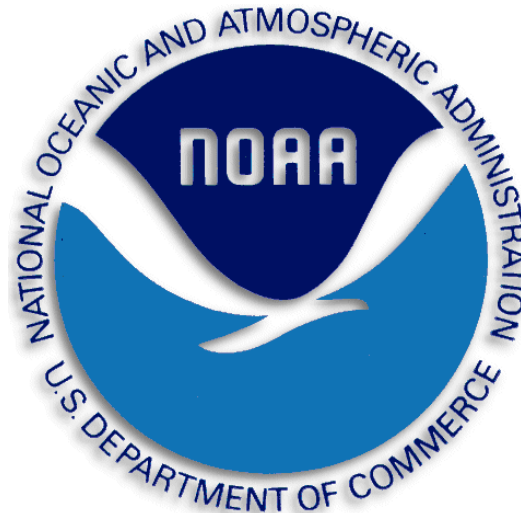


# **NOAA/NESDIS**

## **NESDIS Contingency Planning 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

NESDIS Contingency Planning Policies and Procedures .....	6
Record of Changes/Revisions.....	6
1.0 Background and Purpose .....	2
2.0 Scope.....	2
3.1 Roles, Responsibilities, and Coordination .....	2
3.2 Authorizing Official (AO).....	3
3.3 Chief Information Officer (CIO) .....	3
3.4 Information Technology Security Officer (ITSO).....	3
3.5 System Owner (SO) .....	4
3.6 Information System Security Officer (ISSO).....	4
4.0 Management Commitment.....	4
5.1 Compliance.....	4
5.2 References.....	5
6.1 Policy .....	5
6.2 Policy Maintenance .....	5
6.3 Policy Feedback Process.....	5
6.4 Policy Effective Date.....	5
7.1 Procedures .....	5
7.2 Business Impact Analysis (BIA) .....	7
7.3 Risk Assessment and Preventive Controls.....	8
7.4 Recovery Strategy Development.....	8
7.5 Contingency Plan Development .....	9
7.6 Testing/Exercising .....	9
7.7 Personnel Training .....	10
7.8 Plan Maintenance .....	11
7.7.1 Updating Contingency Planning Status in CSAM.....	11
Appendix A – Preventive Controls Checklist .....	14
Appendix B – Procedures Checklist.....	15
Appendix C – Contingency-Related Plans Checklist .....	16
Appendix D – Test Elements Checklist .....	17


Appendix E – Contingency Planning Artifacts Checklist ..... 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/IT 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

NESDIS Quality Procedure [NQP] – 3406  
Revision 2.2

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Expiration Date: Until Superseded

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, 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](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](mailto:Nancy.DeFrancesco@noaa.gov) or phone (301) 713-1312.

## NESDIS Contingency Planning Policies and Procedures

### Record of Changes/Revisions

Version	Date	Section	Author	Change Description
0.1	August 14, 2009	All	Noblis	First Draft
0.2	September 10, 2009	All	N. DeFrancesco	Updated for Information Technology Security Officer (ITSO) comments
0.3d	January 30, 2010	1.0, 2.0, 7.1, 7.2, 7.7, 7.7.1	N. DeFrancesco	Updated for Information Resource Management Team (IRMT) Security Team comments
0.4d	May 12, 2010	3.4, 3.5, 7.7	Noblis	Updated based on National Climatic Data Center (NCDC) comments; removed the Cyber Security Assessment and Management (CSAM) Appendix L reference
0.5d	June 30, 2010	3.1, 5.1, 7.0, 7.1	Noblis	Minor changes to streamline the process
0.6d	July 14, 2010	Cover, 3.2, 3.3	N.DeFrancesco	Minor edits; specify that the AODR approves the CP on behalf of the AO, specify to use NESDIS templates and checklists.
1.0	August 20, 2010	All	N.DeFrancesco	Finalize and prepare for issuance

Version	Date	Section	Author	Change Description
1.1d	October 31, 2011	1.0, 4.0, 5.1, 6.3, 7.0, 7.1, 7.2, 7.4, 7.5, 7.6, 7.7, 7.7.1, Appendix E	Noblis	Annual review and update to reference latest DOC and NESDIS policies and procedures
1.2d	November 28, 2011	6.1, 7.6	Noblis	Change CP P&P review schedule to bi-annually; the timeline for notifying personnel with significant roles is 30 days.
1.3d	December 7, 2011	All	A. Kuhn	Minor Technical Edits throughout document; added slight procedural change in Section 7.7.
1.4d	January 3, 2012	7.7	A. Kuhn	Added language to allow unsigned CP to be submitted for compliance review
2.0d	May 31, 2012	Version numbering and date	N. DeFrancesco	Accept all changes 1.1d-1.4d and finalize for CIO approval and issuance.
2.1f	September 28, 2012	All	N.DeFrancesco	Finalize and prepare for CIO issuance

## 1.0 Background and Purpose

This document establishes the National Environmental Satellite, Data, and Information Service (NESDIS) Contingency Planning Policy and provides the step-by-step procedures for implementing the contingency planning security controls within NESDIS as outlined in the National Oceanic and Atmospheric Administration (NOAA) *Information Technology (IT) Security Manual 212-1302* (March 31, 2008). By developing a Contingency Planning Program, NESDIS complies with the NOAA Policy, as well as the Department of Commerce (DOC) *IT Security Program Policy (ITSP)* (January 2009).<sup>1</sup>

The National Institute of Standards in Technology (NIST) Special Publication (SP) 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* (August 2009) identifies the security controls in the Contingency Planning family. Additional guidance is provided by NIST in SP 800-34, Revision 1, *Contingency Planning Guide for Information Technology Systems* (May 2010). Selection of the security controls baseline is based on the security categorization and determination of system impact levels (Low, Moderate, or High) as outlined in the Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*.

In this document, NESDIS supplements the NIST SP 800-53 and SP 800-34 guidance by detailing procedures and establishing responsibilities for developing and maintaining a Contingency Plan, as well as training, testing and exercising the Contingency Plan.

Managing a Contingency Planning Program and records in the Cyber Security Assessment and Management (CSAM) tool within NESDIS is also addressed.

## 2.0 Scope

The scope of this document focuses on establishing the foundation for a NESDIS Contingency Planning Program. It specifies responsibilities of key personnel and provides step-by-step procedures for how to develop and manage a Contingency Planning Program.

This document does not replace the NOAA or DOC applicable policies or the associated guidance provided by NIST. Rather, this document provides NESDIS-specific procedures for implementing a Contingency Planning Program and should be used as a companion document for implementation of NIST SP 800-53 and SP 800-34 within NESDIS.

## 3.1 Roles, Responsibilities, and Coordination

This section details NESDIS personnel responsibilities in contingency planning. It supplements the “Assignment of Responsibility” section under the NOAA *IT Security Manual 212-1301* Version 4.2.

---

<sup>1</sup> The DOC ITSP mandates that DOC operational units “develop, document, and implement an IT Security Program to protect the confidentiality, integrity, and availability of DOC information and information systems in accordance with the Federal Information Security Management Act (FISMA) of 2002 and other applicable legislation.”



### **3.2 Authorizing Official (AO)**

The AO has the overall responsibility for ensuring that adequate resources are provided to support operations of NESDIS systems under their responsibility, including resources for adequate contingency planning, testing, and training. On an annual basis, the AO reviews and approves the system's Contingency Plan in writing, after consideration of residual risks (risks that cannot be mitigated through the current Contingency Plan). The AO may delegate Contingency Plan written approval to the AO's Designated Representative (AODR). The AO must also approve all high-risk Plans of Action and Milestones (POA&Ms) to mitigate unacceptable risk associated with the Contingency Plan.

### **3.3 Chief Information Officer (CIO)**

The NOAA Assistant CIO for Satellite and Information Services is responsible for ensuring a Contingency Planning Program is developed and implemented and that the program is in compliance with federal law and DOC/NOAA IT security policies, standards, and practices. The CIO appoints the NESDIS Information Technology Security Officer (ITSO) to oversee the Contingency Planning Programs for all NESDIS systems. The CIO, as the Authorizing Official Designated Representative (AODR) for High-impact systems, can approve the Contingency Plan for High-impact systems on behalf of the AO.

### **3.4 Information Technology Security Officer (ITSO)**

The NESDIS ITSO oversees compliance with the NESDIS Contingency Planning Program on behalf of the CIO. The ITSO shall:

- Establish and maintain the NESDIS Contingency Planning Policy and Procedures;
- Ensure that updates of Contingency Plans, Contingency Plan tests and results, and training programs are completed annually;
- Track the progress of remedial actions on the contingency planning-related POA&Ms;
- Disseminate current information on contingency-related laws, DOC/NOAA IT security policies, regulations, guidelines, and concerns;
- Ensure that adequate and appropriate preventative controls are in place and that the program integrates fully into the NESDIS enterprise architecture, capital planning, and investment control processes;
- Provide guidance and technical assistance on contingency planning; and
- Monitor and provide reports on compliance to AOs and other interested parties.

The ITSO, as the AODR for Moderate-impact systems, can approve the Contingency Plan for Moderate-impact systems on behalf of the AO or co-AOs.

### **3.5 System Owner (SO)**

The SO must develop and maintain a system Contingency Planning Program in accordance with this policy and procedures. The SO shall:

- Develop and update a Contingency Plan at least annually, and obtain AO approval of the Contingency Plan;
- Conduct a Business Impact Analysis (BIA) and risk assessment;
- Implement preventive controls to minimize risks;
- Conduct contingency testing and exercising that includes, but is not limited to, failover/recovery procedures, backup media, alternate equipment, and alternate site;
- Develop a contingency test plan, and record test results in the Contingency Test Plan and Test Results document;
- Initiate necessary agreements (i.e., Service Level Agreements [SLAs], Memoranda of Understanding [MOUs]) to support Contingency Plan implementation;
- Develop a training program to support awareness training for all personnel, and provide specialized training for essential personnel with responsibilities to execute the Contingency Plan; provide records of training to the NESDIS ITSO;
- Support contingency planning annual continuous monitoring activities; and
- Ensure the availability of documentation and necessary artifacts.

### **3.6 Information System Security Officer (ISSO)**

The ISSO supports the SO, as tasked, in any or all contingency planning activities (see a listing of activities in section 3.4 above).

## **4.0 Management Commitment**

The NESDIS Chief Information Division (CID) supports the NESDIS Assistant Administrator's (AA) strong emphasis on securing NESDIS information and information systems including ensuring that Contingency Plans are in place to minimize unacceptable disruption of critical services delivered via NESDIS information systems. Through the issuance of this policy, the CID demonstrates its commitment to providing procedures for managing effective and well-tested Contingency Plans.

### **5.1 Compliance**

The NESDIS ITSO monitors—through periodic quality reviews and monthly performance metrics—implementation of the contingency planning process within NESDIS to ensure compliance with applicable laws, directives, policies, and guidance. The ITSO reports monthly to the AA and reports to the CIO and Office Directors as necessary, but at least monthly, 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, ITSO, SO, or ISSO.

## 5.2 References

- DOC *IT Security Program Policy* (ITSPP) section 4.6 (January 2009)
- DOC Commerce Interim Technical Requirements CITR-006, Version 5.0, *Information System Security Training for Significant Roles* (September 2010)
- DOC Commerce Information Technical Requirements CITR-015, *Contingency Plan Testing and Exercise Activities* (July 2011)
- NOAA *IT Security Manual* 212-1302 (March 2008)
- NIST SP 800-34, Revision 1, *Contingency Planning Guide for Information Technology Systems* (May 2010)
- NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* (August 2009)
- *NESDIS IT Security Handbook*

## 6.1 Policy

To comply with DOC policy, NESDIS AOs shall ensure that SOs develop, document, and implement a Contingency Planning Program to protect the availability of NESDIS information and information systems. NESDIS requires that SOs annually update Contingency Plans, test the contingency capabilities, and train personnel on contingency planning responsibilities. The NESDIS ITSO shall oversee compliance with this policy, keep records of Contingency Plan training, and maintain the policy and procedures.

## 6.2 Policy Maintenance

The NESDIS ITSO shall review the 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.hq.secteam@noaa.gov](mailto:nesdis.hq.secteam@noaa.gov) regarding any errors found in the document or other clarifications or updates that are required.

## 6.4 Policy Effective Date

This policy and the procedures contained herein are effective upon issuance.

## 7.1 Procedures

This section discusses the step-by-step procedures for implementing a Contingency Planning Program within NESDIS. Figure 1 depicts all contingency planning activities that

must be completed to comply with this policy. The initial step is to perform a BIA, which provides a clear understanding of what critical functions, processes, and/or systems need to be protected. The findings of the BIA serve as the criteria in the next step – Recovery Strategy Development. The Contingency Plan Development step incorporates Risk Assessment/Preventive Controls considerations to eliminate or mitigate unacceptable risks identified in the risk assessment.

After documenting the Contingency Plan, the next step is to validate it through Testing/Exercising using documented Test/Exercise Plans with well-defined test objectives. In addition, Personnel Training is vital to ensure that supporting personnel possess the requisite knowledge to execute the Contingency Plan. Next, all lessons learned and recommendations generated from testing/exercising and training must be included in the Contingency Plan and POA&Ms (as necessary). Finally, Plan Maintenance ensures that the content is up-to-date and is always in a “ready-to-execute” mode.

To meet documentation requirements discussed in these procedures, NESDIS SOs shall follow the practices described in the latest version of the NIST SP 800-34 to develop a Contingency Plan and shall use the NOAA/NESDIS contingency planning templates and checklists for documenting contingency planning, including: a *BIA* template; a *Contingency Plan* template; a *Contingency Plan Test Plan and Test Results* template; a *BIA Compliance Review Checklist*; a *Contingency Plan Compliance Review Checklist*, and a *Contingency Plan Test Plan and Test Results Review Checklist* (for compliance assessment). NESDIS has modified these templates and checklists for use NESDIS-wide and they can be found on the NESDIS IT Security Handbook website at:  
[https://intranet.nesdis.noaa.gov/ocio/it\\_security/handbook/it\\_security\\_handbook.php](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/it_security_handbook.php).

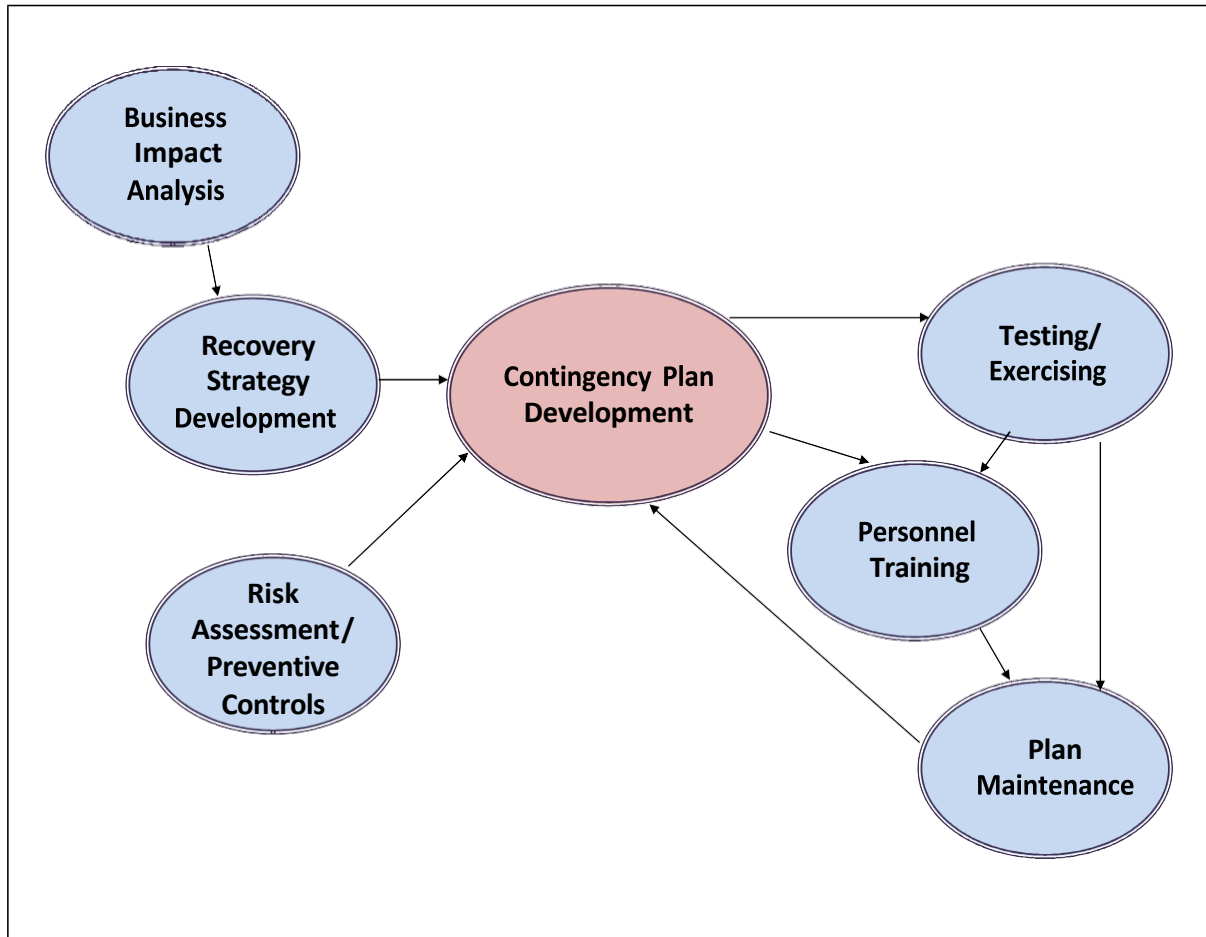


Figure 1 – Contingency Planning Cycle

## 7.2 Business Impact Analysis (BIA)

Conducting a BIA is the first step in contingency planning development. The process is to associate specific systems with the critical functions/services that they provide. Based on the severity of consequences caused by a system failure (which translates into functions/services disruptions), a SO can determine the system criticality and the allowable downtime (Recovery Time Objectives (RTOs)). A recovery strategy can then be developed to ensure the resumption of critical functions within the RTOs.

The BIA report must be validated annually (or sooner for any major system and/or organizational changes). NESDIS requires the use of the BIA template found on the NESDIS IT Security Handbook website at [https://intranet.nesdis.noaa.gov/ocio/it\\_security/handbook/final\\_docs/NOAAAnnnn\\_BIA\\_Template\\_V3.1\\_2011\\_12\\_9\\_NESDIS.doc](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/final_docs/NOAAAnnnn_BIA_Template_V3.1_2011_12_9_NESDIS.doc). The BIA shall be submitted as an artifact, along with the annual submission, as part of the CSAM artifact uploads.

To conduct a BIA, the SO must:

- Follow the instructions in the template and complete the BIA template;

- Verify the adequate and quality completion of the BIA using the BIA Compliance Review Checklist;
- Establish the RTO based on the BIA; and
- Brief the AODR or ITSO on the BIA results upon request, and seek AO or AODR approval of the recommended RTO.

### 7.3 Risk Assessment and Preventive Controls

Under the NESDIS *Continuous Monitoring Planning Policy and Procedures*, a risk assessment through security controls analysis must be conducted annually as part of the three-year cycle to identify vulnerabilities. To support the Contingency Plan, the annual risk assessment must specifically evaluate the contingency planning preventative controls. Appendix A presents a list of preventive controls extracted from the Contingency Planning family and Physical and Environmental Protection family in NIST 800-53 guidelines.

To determine and document the preventative controls, the SO must:

- Ensure security controls associated with the Contingency Plan are reviewed and properly assessed in the context of the BIA and approved Contingency Plan;
- Use the baseline controls as listed in the checklist (Appendix A) and augment the list based on the system environment;
- Complete the tailored preventive controls checklist (Appendix A);
- Develop implementation plans and POA&Ms<sup>2</sup> as necessary; and
- Incorporate preventive controls in the system Contingency Plan, and update the System Security Plan as necessary to reflect all changes in controls implementation.

### 7.4 Recovery Strategy Development

A recovery strategy is the core of a system Contingency Plan. The SO shall evaluate and decide on a variety of recovery options to ensure the approved RTOs (derived from section 7.1) are met.

Based on the results of the BIA, the SO shall gather information on all possible recovery options as well as associated costs. Refer to NIST 800-34 guidance and NIST 800-53 CP controls for definitions and considerations in evaluating and selecting the following key recovery elements, including:

- Selecting an *Alternate Processing Site* and determining an appropriate level of operational readiness;

---

<sup>2</sup> See NESDIS *Plan of Action and Milestones Management Policy and Procedures* - [https://intranet.nesdis.noaa.gov/ocio/it\\_security/handbook/POAM\\_Management\\_PP\\_v1.1\\_091409.pdf](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/POAM_Management_PP_v1.1_091409.pdf) for more information.

- Establishing or validating a Backup Program that provides the best protection to system applications and data;
- Establishing an Alternate Storage Site for storing backup media and other vital records; and
- Evaluating and securing the appropriate level of Telecommunications redundancy.

The SO shall submit the recommended recovery strategy, together with the cost and implementation timeline, to the AO for approval.

## 7.5 Contingency Plan Development

The Contingency Plan development combines the following four elements:

1. Essential functions and RTOs from the BIA in section 7.1;
2. Preventive controls to be implemented as identified from the activities described in section 7.2;
3. Optimal recovery strategy identified from the activities described in section 7.3; and
4. Procedures that must be established to clearly instruct the SO, ISSO, and other system personnel on the necessary actions to implement the Contingency Plan.

For the procedures element, SOs shall complete the *Procedures Checklist* (Appendix B) to ensure that all proper procedures are fully documented in the Contingency Plan. In addition, NIST 800-53 states that the system Contingency Plan shall coordinate the entire suite of emergency management and contingency planning plans associated with that system. SOs shall complete the *Contingency-Related Plans Checklist* (Appendix C) to ensure that all the related plans and the owners are identified.<sup>3</sup> Any related plans shall be uploaded to the CSAM system as contingency planning artifacts.

Contingency Plans for new systems must be approved by the AO and submitted to the Certification Agent for assessment as part of the system Assessment and Authorization (A&A) process.<sup>4</sup> The Contingency Plan shall be in place when the new system is operational. For existing systems, the SO updates the Contingency Plan annually and submits it to the NESDIS ITSO for review. The CP and related documents will serve as artifacts during the annual controls assessment.<sup>5</sup>

## 7.6 Testing/Exercising

Testing/exercising plays a crucial role in validating a Contingency Plan. Testing identifies plan deficiencies and tests the ability of personnel to execute emergency

---

<sup>3</sup> Full definitions of these plans can be found in NIST SP 800-34.

<sup>4</sup> See the NESDIS *Risk Management Framework Assessment and Authorization Process Policy and Procedures* for more information.

<sup>5</sup> See the NESDIS *Policy and Procedures for Conducting Security Controls Assessments* for more information.

and recovery procedures. SOs must use the *Contingency Plan Test Plan and Test Results* template to document contingency testing.

Refer to NIST 800-34 for different types of contingency tests. Testing/exercising must be conducted **annually** or more frequently as determined by the SO or directed by the AO. SOs must use Appendix D to evaluate the adequacy of the testing baseline. SOs may customize the checklist according to the system's specific environment. Tabletop exercise cannot be the only form of contingency exercise for Moderate- or High-impact systems.<sup>6</sup>

## 7.7 Personnel Training

Designated personnel shall be informed in writing of their disaster recovery/business resumption and restoration responsibilities within 30 business days of appointment, and the role-based training must be completed within 60 days of appointment and **annually** thereafter.<sup>7</sup> SOs must develop a procedure to provide initial training and subsequent refresher training. SOs shall use the NESDIS contingency training package (under development) with guidance and templates in developing their system contingency training. The training package is located on the NESDIS IT Security Handbook website at:

[https://intranet.nesdis.noaa.gov/ocio/it\\_security/handbook/it\\_security\\_handbook.php](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/it_security_handbook.php).

Training shall involve the following personnel:

- Personnel who are responsible for activating the Contingency Plan and monitoring crisis in an emergency situation
- Personnel to conduct damage assessment
- Personnel who will be deployed (or relocated) to an alternate processing site
- Personnel supporting reconstitution (or restoration) of the primary system at the impacted site

Personnel shall be trained on the following plan elements:

- Purpose of the plan
- Notification procedures and communications plan
- Contingency Plan activation process and who has the authority to activate the plan
- Security requirements
- Team-specific procedures

---

<sup>6</sup> See CTR-015: *Contingency Plan Testing and Exercise Activities* for more information on the latest DOC requirements.

<sup>7</sup> See the NESDIS *IT Security Training Policy and Procedure* for more information on notifying and training personnel appointed to significant IT security roles, and CTR-006: *Information System Security Training for Significant Roles* for minimum hours of requirement.



- Team responsibilities defined in the Contingency Plan
- Crisis event simulations (for high-impact systems)

Upon completion of training, the SO must provide written notification to the NESDIS IT Security Office via e-mail to [nesdis.it.security@noaa.gov](mailto:nesdis.it.security@noaa.gov). In addition, a summary of the training records is required to be posted/updated in Appendix N of the Contingency Plan (see *Contingency Plan* template).

## 7.8 Plan Maintenance

NESDIS requires SOs to review and revise (if necessary) system Contingency Plans **annually**. Annual updates to the Contingency Plan must consider changes that occurred in the prior 12 months to: documentation requirements/templates; organization and contingency points of contact information; the information system and its environment of operation; and problems encountered during Contingency Plan implementation, execution, or testing. In addition, a Contingency Plan must be updated upon a significant change to the system, organization goals, and/or personnel assignments, as well as when lessons learned and corrective actions are identified from testing and training.

On an annual basis, SOs shall submit the CP, associated documents including the Business Impact Analysis and Occupant Emergency Plans, and artifacts to the Chief Information Division 60 days prior to the due date for approval. The ITSO shall conduct a quality review of all contingency planning documentation and provide review results to the SO within five business days. ISSOs can submit an unsigned copy of the CP for the compliance review. Any non-complaint issues then need to be resolved and revised. The CP shall then be re-submitted for subsequent review. The CP that has passed the compliance review will be ready for sign off by ISSO, SO, and AODR.

In addition, the documentation, together with contingency activities supporting artifacts, shall be evaluated independently as part of the annual continuous monitoring process.

### 7.7.1 Updating Contingency Planning Status in CSAM

**Step 1.** The DOC has designated the CSAM system to manage its IT Security program. NOAA and NESDIS have adopted this tool, and hence, all NESDIS systems are required to track IT security activities via this system. To record and update contingency planning activities, complete the following steps:

**Step 2.** Logon to CSAM

**Step 3.** Select “SSP Contents”

**Step 4.** Select your system (SSP Name hyperlink)

- Step 5.** Click “Status” on the Menu (under the second level of menu options: SSP List, General, Info Types, Locations, Interfaces, Narratives, Appendices, POCs, Artifacts, RTM, Status, Tools)
- Step 6.** To add or update a Contingency Plan activity:
- a. Click “Edit” on the left side of the SSP Status window
  - b. Under the “Status” field in the “Contingency Plan” row, choose from one of the drop down menu choices: Not Started, In Progress, Completed, Tested, Expired (Plan), Expired (Test), Expired (Both), or Not Applicable
  - c. Provide a date in the “Initiated” field at the start of Contingency Plan development or review cycle.
  - d. Provide a completion date in the “Date Completed” field upon receipt of a signed Contingency Plan.
  - e. Provide the one year anniversary date of the signed/approved Contingency Plan under “Next Due Date” (this date is exactly 12 months/365 days from the test completion date).
  - f. No update is required under the “Expiration Date” field.
  - g. Click “Update” on the left side of the SSP Status window
  - h. Upload a signed PDF copy of the Contingency Plan under “Artifacts” field in the Contingency Plan row of the Status page. Upload all relevant CP artifacts, if applicable.
- Step 7.** To add or update a Contingency Plan test activity:
- a. Click “Edit” on the left side of the SSP Status window.
  - b. No update is required under the “Status” field.
  - c. No update is required under the “Initiated” field.
  - d. Provide the completion date in the “Date Completed” field upon completion of a contingency test.
  - e. Provide the one year anniversary date of the contingency test under “Next Due Date” (this date is exactly 12 months/365 days from the test completion date).
  - f. No update is required under the “Expiration Date” field.
  - g. Click “Update” on the left side of the SSP Status window
  - h. Upload Contingency Plan Test Plan and Test results under “Artifacts” field in the Contingency Plan Test row. Upload all relevant artifacts, if applicable.

It is the responsibility of SOs and their designate(s) to maintain these records and to update the status (and provide dates) within five business days upon the completion of contingency planning activities, but no later than the due date. Appendix E contains a list of contingency-related documents that shall be maintained and reviewed for accuracy at least annually. All applicable documents shall be uploaded to CSAM as artifacts. When applicable, multiple artifacts can be uploaded. If a given artifact is used to satisfy a POA&M, the POA&M has a procedure to reference this artifact (there is no need to upload a document twice).

The ITSO and ITSO staff monitor security controls (including contingency planning controls) through CSAM.

### Appendix A – Preventive Controls Checklist

Control No.	Control	Implementation Status (Yes, No, N/A)	Risk Description
CP-6	Alternate Site Storage		
CP-7	Alternate Processing Site		
CP-8	Telecommunications Services		
CP-9	Information System Backup		
CP-10	Information System Recovery and Reconstitution		
PE-2	Physical Access Authorizations		
PE-3	Physical Access Control		
PE-4	Access Control for Transmission Medium		
PE-5	Access Control for Output Devices		
PE-6	Monitoring Physical Access		
PE-7	Visitor Control		
PE-8	Access Records		
PE-9	Power Equipment and Power Cabling		
PE-10	Emergency Shutoff		
PE-11	Emergency Power		
PE-11 (1)	Gasoline- or Diesel-powered Generators (for high-impact system)		
PE-12	Emergency Lighting		
PE-13	Fire Protection		
PE-14	Temperature and Humidity Controls		
PE-15	Water Damage Protection		
PE-16	Delivery and Removal		
PE-17	Alternate Work Site		
PE-18	Location of Information System Components		

### Appendix B – Procedures Checklist

Type of Procedure	Check (if exists)	Procedure Author
Personnel Notification		
System Contingency Plan Activation		
Alternate Processing Site Activation		
Alternate Equipment Activation		
Backup Media Retrieval Procedure from the Alternate Storage Site		
System Failover Procedures		
System Operations at Alternate Processing Site (if different from normal operations)		
Backup procedures at Alternate Processing Site (if different from normal operations)		
System Restoration Procedures		
Cutover Procedures for Returning from Alternate Processing Site to Primary Site		
Alternate Processing Site Stand-down Procedures		

### Appendix C – Contingency-Related Plans Checklist

Type of Plan	Name of the Plan (if exists)	Plan Owner
Continuity of Operations Plan to address organizational and facility level contingency planning		
Business Continuity Plan or Business Resumption Plan to address contingency planning for business processes		
Disaster Recovery Plan to address IT-focused plan to restore system operability		
Occupant Emergency Plan to focus on personnel safety with procedures to direct personnel to safety		
Crisis Communications Plan to ensure communications both internally and externally (general public, customers, vendors, etc.)		
Cyber Incident Response Plan to address cyber attacks		
Other IT or System Contingency Plan(s) that are owned by the same organization. Please list: 1) 2)		
Other IT or System Contingency Plan(s) that are connecting to this system. Please list: 1) 2)		

### Appendix D – Test Elements Checklist

Test Element	Completion Status (Yes, No, N/A)
Organization call tree notification	
Standing up a Command Center and coordination among different “disaster recovery” teams	
Retrieval of backup media from an off-site storage location	
Restoration of backup media	
Alternate processing site deployment	
Activation of alternate equipment	
Failover procedures	
Redundant circuit(s) testing	
Telework exercise	
Restoration procedures	
Backup generator activation	
Simulation of a full recovery and restoration of system (for high impact system)	

**Appendix E – Contingency Planning Artifacts Checklist**

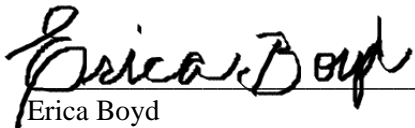
Artifact	Document Name	Last Review Date
BIA		
BIA Checklist		
System Contingency Plan		
System Contingency Plan Checklist		
Contingency Plan Test Plan and Test Results		
Contingency Plan Test Plan and Test Results Checklist		
Personnel Training Records		
Procedures Checklist		
Test/Exercise Completion Checklist		
Off-site Storage Agreement or MOU		
Alternate Processing Site Agreement or MOU		
Telecommunications SLA		
Hardware Vendor SLA(s)		
Software Vendor SLA(s)		
Other Contingency Planning related Plan(s) Please list:		



## Approval Page


Document Number: NQP-3406, Revision 2.2	
Document Title Block: <b>NESDIS Contingency Planning Policy and Procedures</b>	
<b>Process Owner:</b> 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-3406