NOAA/NESDIS

Continuous Monitoring 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

UNITED STATES DEPARTMENT OF COMMERCE
National Oceanic and Atmospheric Administration
NATIONAL ENVIRONMENTAL SATELLITE. DATA AND INFORMATION SERVICE
Siler Spring, Maryland 209 10

September 30, 2012

MEMORANDUM Distribution

FOR: 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 /111erconnections*, v2.1;
4. NESDIS *Contingency Planning Policy and Procedures*, v2. 1;
5. NESDIS *Policy and Procedures for Ensuring Security i11 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 .l ;
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 011 NESDIS Information Systems*, v3.l.

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, 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 Nancv.DeFrancesco@noaa.2ov or phone (30I) 713-1312.

NESDIS Continuous Monitoring Planning Policy and Procedures

Record of Changes/Revisions

Version	Date	Section	Author	Change Description
Draft 1.0	7/24/2009	All	Noblis	Initial Draft Version for OCIO review
Draft 1.1	8/20/2009	All	ITSO	Update for ISSO comments
Pre-final Draft 1.2	9/15/2009	7.1.7	ITSO	Update for NESDIS-wide comments and issue pre-final draft for comment
Final v1.0	9/30/2009	Date	ITSO	Issue in final
Draft 2.0	3/8/2012	All	ITSO Support Staff	Annual Update
Final 2.1	9/28/2012	All	NESDIS ITSO	Finalize changes and route for CIO issuance

1.0 Background and Purpose

The Federal Information Security Management Act ([FISMA], 44 U.S.C. § 3541, *et seq.*), and the Office of Management and Budget Circular A-130 Appendix III require management authorization (accreditation) of all information systems to store, process, or transmit federal data. The Department of Commerce (DOC) *Information Technology Security Program Policy* (ITSPP) requires compliance with National Institute of Standards and Technology (NIST) guidance, specifically NIST Special Publication (SP) 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, for implementing the security Assessment and Authorization (A&A) process. NIST SP 800-37 Revision 1 establishes the Continuous Monitoring requirement to ensure oversight and monitoring of security controls in the information system on an ongoing basis and that the authorizing official is informed when changes occur which may impact the security of the system.

An effective Continuous Monitoring Plan (Plan) can substantially reduce the National Environmental Satellite, Data, and Information Service (NESDIS) costs and level of effort required for system re-accreditations. To achieve the highest degree of cost effectiveness, a NESDIS-specific standardized approach to developing and implementing Plans is required.

The purpose of this document is to communicate NESDIS-specific policy and procedures for effectively implementing a continuous monitoring planning and reporting process.

2.0 Scope

The scope of this document is limited to establishing the NESDIS requirement for Plans and to provide procedures for how to (1) comply with NESDIS requirements for distributing controls across the three year continuous monitoring cycle of annual assessments, and (2) determine/document the NESDIS compliant due date for continuous monitoring and reporting. This document does not provide detailed instructions for conducting continuous monitoring assessment activities. See the *NESDIS Policy and Procedures for Conducting Security Controls Assessments* for such guidance.

All NESDIS employees and contractors responsible for conducting continuous monitoring activities for NESDIS information systems, including contractor-owned and -operated systems which contain NESDIS information, must comply with the policies and procedures identified in this document.

3.0 Roles, Responsibilities, and Coordination

The roles and responsibilities for key participants involved in continuous monitoring for NESDIS systems are consistent with those described by NIST. Participants in the continuous monitoring process and their roles and responsibilities are listed below.

3.1 NESDIS Assistant Administrator (AA)

The NESDIS AA serves as the Chief Executive Officer with overall responsibility to provide information security protections commensurate with the risk and magnitude of harm (i.e., impact) to organizational operations and assets, individuals, other organizations, and the Nation resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of: (i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

3.2 Authorizing Official (AO)

The AO shall review the results of all Continuous Monitoring Assessment Reports and approve Plans of Action and Milestones (POA&Ms) created as a result of the assessment.

3.3 System Owner (SO)

The SO is responsible for meeting all NESDIS-specific continuous monitoring planning and reporting requirements identified in the document. The SO may delegate continuous monitoring activities to the Information System Security Officer (ISSO). The SO must maintain a Plan in Appendix H of the System Security Plan (SSP).

3.4 Common Control Provider (CCP)

NESDIS uniquely establishes the role of CCP. The CCP is responsible for meeting all NESDIS-specific continuous monitoring planning and reporting requirements identified in this document as SO responsibilities, except as applicable for all common controls for which they have operational control. The *NESDIS Common Control Policy and Procedures* (under development) will provide more information on the responsibilities of a NESDIS CCP.

3.5 Information System Security Officer (ISSO)

The ISSO is responsible for maintaining the security posture of the system in accordance with the SSP and is also responsible for assisting with continuous monitoring and reporting activities, as tasked by the SO.

3.6 Chief Information Officer (CIO)

The NOAA Assistant CIO for Satellite and Information Services establishes and oversees the NESDIS-specific continuous monitoring program and advises executive leadership regarding the security risk associated with continuous monitoring results reported.

3.7 Information Technology Security Officer (ITSO)

The NESDIS ITSO is responsible for establishing, implementing, and maintaining the NESDIS continuous monitoring planning requirements.

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. Through the issuance of this policy and procedures document, the CID demonstrates its commitment to the consistent, comprehensive, and cost effective continuous monitoring for every NESDIS system.

5.0 Compliance

The NESDIS ITSO monitors – through periodic SSP compliance reviews and monthly performance metrics – the implementation of the continuous monitoring process 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.

5.1 References

- DOC ITSPP section 4.4.7 (January 2009)
- Commerce Information Technology Requirement 019, *Risk Management Framework (RMF)* (July 2012)
- NOAA *Continuous Monitoring Guidance for Annual Security Control Assessments* (v4, February 2012)

6.0 Policy

As required by DOC ITSPP section 4.4.7, the NESDIS-specific continuous monitoring process and procedures shall align with the DOC- and NOAA-prescribed practices for implementing an effective continuous monitoring planning process. It should be used as a companion document for implementing the sixth step of the assessment and authorization process as described by NIST SP 800-37, Revision 1, and not as a replacement document.

6.1 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.

6.2 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.

6.3 Policy Effective Date

This policy is effective within 30 days of issuance.

7.0 Procedures

NESDIS requires that the SO maintain a Continuous Monitoring Plan and an Assessment and Authorization (A&A) project plan as living documents. Templates, along with DOC and NOAA guidance for continuous monitoring can be found on the NESDIS IT Security Handbook website at: https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/it_security_handbook.php. See section 7.1 for detailed information on what forms shall comprise the Continuous Monitoring Plan (Plan) and section 7.2 for details on maintaining an A&A Project Plan.

The Plan shall be updated at least annually to reflect adjustments associated with assessment results and POA&M closures as they occur throughout each year of the system authorization period and is subject to annual compliance review by the ITSO.[1]

7.1 Scheduling and Distributing Security Controls for Continuous Monitoring

Complete the following steps for initial scheduling and distribution of security controls:

Step 1. Open the Plan Template and update the system name, authorization period, and identifier information.

Step 2. Select the appropriate impact level for the system. The Template automatically populates the Plan with the controls mandated by DOC, NOAA, and NESDIS for annual control assessment which must be assessed at least once in each year of the authorization period, and may not be deferred.

Step 3. After the initial population of the spreadsheet, edit the list of controls to denote controls that have been tailored under the Federal Information Processing Standard 200 approval for the system baseline.

Step 4. Add any controls considered uniquely volatile and critical for the system by the SO to be annually or more frequently assessed, if applicable (see DOC CITR-019 for more information).

Step 5. Review all POA&Ms in the Cyber Security Assessment and Management (CSAM) tool (including those identified by the AO during the authorization briefing) and schedule the assessment of any control expected to be addressed or affected by a POA&M in the year in which the POA&M is scheduled for completion.

Step 6. Finally, distribute the remaining controls which have not been scheduled for assessment across the three year authorization period. NESDIS highly encourages a strategically even distribution of the remaining controls across the authorization period. For example, the SO might choose to assess the implementation of any remaining technical controls throughout the authorization period by testing the implementation of the control on different types of components in separate years. In a large system with a mix of Windows and UNIX systems, the SO could assess the implementation of access controls for the Windows systems one year, and the UNIX systems the next year as long as the control is completely assessed between the authorization cycles.

Annually, SOs must complete the following steps to update the schedule and distribution of the security controls in the Plan:

Step 1. At the beginning of the second and third years of the authorization period, evaluate the list of controls scheduled for evaluation during the current year and determine if any adjustment of the initial schedule and distribution of controls are required, and make revisions accordingly.

Note: Controls for which DOC, NOAA, and NESDIS require mandatory annual assessment must be assessed at least once in *each* year of the authorization period, and may not be deferred.

Step 2. Take advantage of other assessment activities which will be performed during the year and update the Plan schedule to coincide with these events. For example, if a POA&M is scheduled for completion during the assessment year, the SO should take advantage of the POA&M closure assessment to satisfy that control's continuous monitoring requirement for the authorization period (unless it is required for annual assessment by DOC, NOAA, or NESDIS).

Step 3. If an assessment is moved up in the schedule, consider shifting a similar assessment from the current year to that same year. For example, if a POA&M closure entails technical testing of a control implementation, technical testing for another control may be delayed to keep resource requirements balanced.

Note: Assessments which are delayed for this reason shall be given higher priority in their new schedule to ensure that assessments of volatile and/or critical controls[2] are not excessively delayed.

Step 4. Add controls associated with a POA&M that were closed since the previous assessment. Results of assessments performed for verifying the closure of a POA&M shall be submitted as part of that year's continuous monitoring report. Assessments of controls with known failures may be delayed until the failures are corrected, but partial corrections may be formally assessed if the partial correction provides a sufficient improvement to the system's security posture to report the change to the AO. The *NESDIS Policy and Procedures for Conducting Security Controls Assessments* provides additional details on the factors to consider when selecting controls for continuous monitoring.

7.2 Maintaining an A&A Project Plan

The SO must maintain an A&A Project Plan using the template available on the NESDIS IT Security Handbook website at: https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/it_security_handbook.ph. The Project Plan must be updated at least annually after completion of all continuous monitoring activities for the fiscal year and must be filed with the System Security Plan (SSP) Core Documents as an element of SSP Appendix H.

7.3 Reporting Procedures

Step 1. NESDIS requires the SO to document, annually update, and submit a Plan and A&A Project Plan and maintain them in the SSP at Appendix H, and upload to the system security authorization package in the CSAM system. The Plans shall provide the SO with an approach to ensure all system security controls are tested at least once during the authorization period as required by NESDIS, or more frequently as determined by the SO, and that all A&A continuous monitoring activities are properly planned for completion during the fiscal year.

Step 2. The NESDIS ITSO shall provide a compliance review and approval of all Plans as part of the annual SSP compliance review. The ITSO shall review and provide compliance assessment results to the SO within 10 business days from the date of receipt of the SSP core documents package by the ITSO. Comments on the acceptability of the Plan will be addressed in the SSP compliance review report provided to the SO. Upon development of the security assessment plan for the annual assessment, the ITSO shall discuss control selection revision recommendations with the SO, update the Plan to reflect modifications agreed to for the current year assessment, and adjust the control selection for future years accordingly. In the event that the SO and ITSO cannot agree on the Plan, they will meet together with the AO to discuss the differences in their assessments. In all cases of conflicts, the AO will have final determination and approval authority of controls selected for assessment through the annual approval of the SSP.

Step 3. NESDIS requires that the SO submit the final annual Security Authorization Package (Package) to the ITSO on or before the annual Security Controls Assessment (SCA) start date, in accordance with the schedule maintained in the CID Monthly Status Review slides.

Step 4. After completion of the SCA by CID, the SO transmits the annual Security Authorization Package to the AO/coAOs for acceptance of risk and system re-authorization. The Package transmittal (Appendix A) references the AO-approved SSP on file in CSAM, and conveys a summary of the results and POA&Ms from the current year's annual SCA. The SO must coordinate submission of their annual Package with the ITSO beginning 15 calendar days prior to the due date to allow sufficient time for Package review and processing for AO re-authorization approval.

Step 5. The ITSO will perform a quality review and provide feedback to the SO within five business days from receipt of the Package. If the Package is determined to be acceptable by the ITSO, the ITSO will document an independent Certifier's recommendation in a memo or in the Security Assessment Report. If the Package is determined to be inadequate or incomplete, the ITSO will coordinate with the SO to resolve deficiencies. In the event that the SO and ITSO cannot agree on the content of the Package (such as disagreement with the POA&M remediation strategy proposed or level of residual risk), they will meet together with the AO to discuss the differences. In all cases, the AO will make the final risk determination and authorization decision.

Step 6. If requested by the AO, the SO, assisted by the Certifier, must communicate to the AO the results of the assessment and level of residual risk, and obtain AO approval of all POA&Ms created as a result of the assessment. An example of an SO transmittal memo is provided in Appendix A. Written notification must be provided to the ITSO to reflect that the AO was informed of the assessment results (either by hard copy or oral presentation) and that the AO approved the POA&Ms associated with the assessment results.

APPENDIX A: System Owner Notification Memorandum

[Instructions: Copy the below text to a separate document, complete all shaded areas, remove highlighting before presenting to AO for signature on agency letterhead.]

<Date>

MEMORANDUM FOR: <Authorizing Official name>
<Title, Office>

FROM: <System Owner name>
<Title, Office>

Subject: FY20xx Annual Security Authorization Package for the <System long title> (NOAA50xx)

The required annual security assessment of the <System long title> (System Acronym), System ID NOAA50xx, operating in <location(s)>, has been conducted by the NESDIS Chief Information Division in accordance with federal requirements. The residual risk was determined by the NESDIS IT Security Officer (ITSO) to be <High, *Moderate, Low*>. I recommend that the risk is acceptable and that you sign the enclosed memo (1) reaffirming the <ATO date as Month yyyy> authorization to operate (ATO), and (2) approving the attached Plan of Action and Milestones (POA&M). The POA&Ms describe the corrective measures to reduce or eliminate newly discovered vulnerabilities that are planned to address deficiencies in the security controls.

The Security Authorization Package provided for your review includes: the System Security Plan (SSP) on file in the Cyber Security Assessment and Management system, an executive summary of the final security assessment report (attachment 1), the NESDIS Authorizing Official's Checklist (attachment 2), and the POA&Ms created to address unacceptable deficiencies in system controls that were assessed in FY20xx (attachment 3).

The assessment was performed in accordance with the National Institute of Standards and Technology (NIST) Assessment & Authorization (A&A) continuous monitoring process that is based on Office of Management and Budget Circular A-130, Appendix III, *Security of Federal Automated Information Resources*; NIST Special Publication 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*; and the Commerce, NOAA, and NESDIS policies and procedures for system security authorization. The ITSO independently assessed selected system components and/or controls documented in the approved SSP. The ITSO used the required NIST assessment methods and procedures to determine the continued extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

If you have any questions or concerns regarding the assessment performance or results, please contact me at (xxx) xxx-xxxx, or the NESDIS ITSO, Nancy DeFrancesco, at (301) 713-1312.

Attachments

cc:
<ITSO Name>/NESDIS/CID

<ISSO Name>/<System Name> ISSO/<System Office>

Approval Page

Document Number: NQP-3402, Revision 2.2	
Document Title Block: **Continuous Monitoring Planning Policy and Procedures**	
Process Owner: NESDIS Chief Information Division	Document Release Date: September 28, 2011

Prepared by:

Erica Boyd 3/25/15

Erica Boyd Date:
Ambit- Associate Consultant
NESDIS Chief Information Office

Approved by:

Irene Parker 3/25/15

Irene Parker Date:
Assistant Chief Information Officer - Satellites

Document Change Record

VERSION	DATE	CCR #	SECTIONS AFFECTED	DESCRIPTION
2.2	**March 25, 2015**	**----**	**ALL**	**Baseline NQP-3402**