NESDIS

Policy and Procedures for Conducting Security Controls Assessment

May 15, 2013

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 Policy and Procedures for Conducting Security Control Assessments

Record of Changes/Revisions

Version	Date	Section	Author	Change Description
Draft 1.0	4/17/2009		Noblis	Initial Draft Version for OCIO review
Draft 1.1	6/18/2009	3.1,3.6, 3,8, 8.1.1, 8.1.6, 8.2.2, 8.3	Noblis	Updates in response to comments.
Draft 1.2	8/15/2009	All	N.DeFrancesco	Update and issue final for NESDIS-wide comment.
Final 1.0	8/31/2009	3.0, 8.3	N.DeFrancesco	Address comments on final draft and finalize for issuance by CIO.
2.0 draft	05/15/2013	all	N.DeFrancesco	Update for new NIST publications and NOAA/NESDIS process changes

1.0 Background and Purpose

The Federal Information Security Management Act [(FISMA), Public Law 107-347] and the Office of Management and Budget (OMB) Circular A-130 Appendix III require management authorization of all information systems to store, process, or transmit federal data. Additionally, OMB Circular A-130 Appendix III requires that management authorization "be based on an assessment of management, operational, and technical controls."

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) 800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*, as the basis for assessing information system security controls to determine the extent to which they are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements. The DOC ITSPP also requires compliance with NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, and NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*. NIST 800-37 identifies the requirements for applying the Risk Management Framework (RMF) and for performing Assessment and Authorization (A&A) of IT systems, including Security Control Assessment (SCA, which is A&A Step 4 and Task 6-2 of Step 6). NIST SP 800-53A addresses security control assessment and continuous monitoring and provides guidance on the security assessment process. NIST SP 800-115 provides guidance on performing security testing, including techniques for identifying active components, but, for example, does not address what comprises an appropriately sized representative sample.

Control assessments are required for several phases of the A&A lifecycle. While each phase has unique requirements to meet its goals, the security control assessment methodology is similar. The purpose of this document is to communicate NESDIS policy and describe the NESDIS-specific process procedures for implementation of the guidance provided in NIST SP 800-53A. Users of this document must also utilize NIST SP 800-53A to fully assess IT Security control implementation for NESDIS systems. This document is not intended to be a stand-alone Control Assessment handbook and intimate knowledge and understanding of NIST SP 800-53A is required to successfully plan and execute control assessments.

2.1 Scope

This policy applies to all personnel, whether government employees or contractors, who perform security control assessments of any NESDIS system as described in Section 7.7.

The scope of this document is to supplement guidance provided by NIST publications, as well as DOC and NOAA policies and procedures with NESDIS specific policies and procedures for the conduct of security control assessments. This policy does not provide detailed guidance on how to develop documents required supporting the process (i.e. SSP, SCA procedures, etc.). Such guidance is provided in NIST Special Publications, including NIST SP 800-53, SP 800-53A, SP 800-18, SP 800-37, SP 800-30, and SP 800-115. It also does not address how to conduct penetration testing or vulnerability assessments, nor does it address the specific execution of NIST SP 800-53A Assessment cases. See the following NESDIS documents for additional guidance:

- NESDIS *Risk Management Framework Assessment and Authorization Process Policy and Procedures*
- NESDIS *Federal Information Processing Standards Publication (FIPS) 199 Policy and Procedures*
- NESDIS *FIPS 200 Security Control Selection and Tailoring Policy and Procedures*
- NESDIS *System Security Plan Development and Maintenance Policy and Procedures*
- NESDIS *Continuous Monitoring Planning Policy and Procedures*
- NESDIS *Plan of Action and Milestones Management Policy and Procedures*
- NESDIS *IT Security Training Policy and Procedures*
- NESDIS *Policy and Procedures for Determining Minimum Documentation Requirements for System Interconnections*
- NESDIS *Annual Risk Assessment Update Interim Technical Guidance*

3.1 Roles, Responsibilities, and Coordination:

NIST SP 800-37 Section 2.2 describes the roles and responsibilities of key participants involved in an agency's security certification and accreditation process. The roles and responsibilities for key participants involved in the assessment of security controls for NESDIS systems are consistent with those described by NIST. Participants in the control assessment process are listed below, along with the following designations/clarifications added by NESDIS for those roles and responsibilities.

3.2 Authorizing Official (AO)

The AO (for high-impact systems) or co-AOs (for moderate-impact systems) shall approve an independent Security Control Assessor (SCA) for performing annual security controls assessments requiring independence. The AO(s) also approve POA&Ms resulting from the assessment and affirm their authorization decision after being briefed by the SO on the assessment results.

3.3 Authorizing Official Designated Representative (AODR)

The NOAA Assistant Chief Information Officer (ACIO) for NESDIS is the AODR for all NESDIS high-impact systems. The NESDIS IT Security Officer is AODR for all NESDIS moderate-impact systems.

3.4 Assistant Chief Information Officer (ACIO)

The NESDIS ACIO serves as AO (in a co-AO capacity) for moderate-impact systems that are not under the direct responsibility of the Chief Information Division (CID).

This role may be delegated to the Deputy ACIO.

3.5 Information Technology Security Officer (ITSO)

The NESDIS ITSO oversees the performance of SCAs for NESDIS IT systems, supported by a team of CID staff and support contractors.

3.6 Certifier

The Certifier oversees SCA performance by the independent SCA team. The Certifier reviews and approves the assessment plan to ensure adequate SCA coverage and depth. The Certifier also reviews reports produced by other independent teams in support of the SO's continuous monitoring activities (such as external penetration test reports, contingency plan tests, etc.). The Certifier verifies and attests to the effectiveness of the security control implementation based on assessment evidence, recommends corrective actions to mitigate deficiencies identified, and provides an opinion regarding the system's residual risk posture and appropriateness for authorization to operate (ATO). The Certifier ensures that NESDIS criteria for SCAs are met.

3.7 System Owner (SO)

The SO performs SCA as part of POA&M closure, annual continuous monitoring, and risk assessment activities.[1] The SO coordinates with the NESDIS ITSO to ensure that the implementation of IT security controls is fully verified for their system in accordance with all applicable guidance. The SO must cooperate with the

independent Certifier and authorize sufficient and appropriate access to the system components and system environment for the SCA to appropriately verify control implementations. The SO shall coordinate with the Certifier to obtain agreement that the team has adequate independence prior to scheduling the assessment, and obtain AO approval and funding of independent SCA services. The SO provides the SCA team all System Security Plan (SSP) Core Documentation necessary for the SCA team to develop a SAP and assess system documentation (see section 9.0).

3.8 Common Control Provider (CCP)

NESDIS uniquely establishes the role of CCP. The CCP is similar to a SO, but is only responsible for the implementation and maintenance of a subset of NIST SP 800-53 controls which will be inherited as common controls by other information systems. The CCP is responsible for the documenting the controls in a security plan,

[1] Any control assessment performed by an independent agent has the highest probability of reuse for security authorization at the Certifier's discretion.

appropriately assessing[2] the controls, documenting the control findings in a Security Assessment Report (SAR), and producing a Plan of Action and Milestone (POA&M) for deficiencies identified during assessments. In addition, the CCP is responsible for providing input to the ITSO on all applicable data calls and reporting requirements.

NESDIS documentation and supporting evidence requirements for A&A of common controls are identical to an information system (i.e. SSP, Risk Assessment, etc.).

Within the context of a set of common controls, the CCP must perform the same responsibilities as an information system owner. Throughout this policy and procedure, all responsibilities of SO also apply to CCP. Common Control Providers using this policy and procedure should assume responsibilities for all SO responsibilities within the context of the identified common controls set.

3.9 Information System Security Officer (ISSO)

NESDIS ISSOs shall:

- Support the SO in:
    - authorizing SCA team's access to the system components and system environment,
    - coordinating scheduling between the SCA team and system personnel, and
    - providing requested documentation to the SCA team.
- Act as the point of contact for the SCA activities.
- Coordinate with the Certifier to ensure that the assessment plan appropriately reflects the controls as described in the SSP and implemented for the system and that the plan adequately and appropriately addresses those controls.
- Support the SO in consulting with the NESDIS ITSO as necessary to ensure adequacy in verifying the controls.

3.10 Security Control Assessment Team

The SCA team is an individual, group, or organization responsible for conducting a comprehensive assessment of the management, operational, and technical security controls in an information system to determine the 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. SCA teams may also provide a risk assessment of the severity of weaknesses or deficiencies discovered in the information system and recommend corrective actions to address identified vulnerabilities in the system. In addition, SCA teams prepare the final security assessment report containing the results and findings from the assessment.

[2] Appropriate assessment refers to the NIST SP 800-53A control assessment of the identified common controls. Common controls utilized for High and Moderate impact systems must be independently assessed. See NESDIS Controls Assessment Policy and Procedure as well as the NESDIS Common Controls Policy and Procedure for more information.

Unless already performed by the Certifier, prior to initiating the security control assessment activities an SCA team must perform compliance review of the SSP Core Documents package to help ensure that the SSP and supporting documentation provide a set of security controls for the information system that is adequate to meet all applicable security requirements. Within NESDIS, the Certifier is responsible for developing the NIST SP 800-53A compliant assessment plan and approving it prior to SCA team execution of the assessment plan.

The required level of assessor independence is determined by the specific conditions of the security control assessment. For example, when the assessment is conducted in support of an authorization decision, the authorizing official makes an explicit determination of the degree of independence required in accordance with federal policies, directives, standards, and guidelines. Assessor independence is an important factor in: (i) preserving the impartial and unbiased nature of the assessment process;

(ii) determining the credibility of the security assessment results; and (iii) ensuring that the authorizing official receives the most objective information possible in order to make an informed, risk-based, authorization decision. The information system owner relies on the security expertise and the technical judgment of the assessor to:

(i) assess the security controls in the information system and common controls inherited by information systems using assessment procedures specified in the security assessment plan; and (ii) provide specific recommendations on how to correct weaknesses or deficiencies in the controls and address identified vulnerabilities.

3.11 System Personnel

System personnel are responsible for cooperating with the performance of the SCA by participating in interviews and demonstrating the operation of implemented controls as requested by the SCA team. System and network administrators shall work with the SCA team to ensure they are granted the authorized access to the system components and system environment. Upon request and with oversight of the SCA team, system and network administrators shall execute assessment procedures documented in the assessment plan requiring direct interaction with the system.

System and network administrators may halt an assessment procedure, and notify the Certifier immediately, if they have reason to believe the assessment will compromise an operational system.

4.0 Management Commitment

The NESDIS CID supports the NESDIS Assistant Administrator’s strong emphasis on securing NESDIS information and information systems. Through the issuance of this policy and accompanying procedures, the CID demonstrates its commitment to the consistent and comprehensive conduct of security control assessments of every NESDIS system.

5.1 Compliance

The NESDIS ITSO monitors—through periodic quality reviews and monthly performance metrics—completion of the security controls assessments within NESDIS to ensure compliance with applicable laws, directives, policies, and guidance. The ITSO reports to the AA monthly, and to the ACIO and Office Directors as necessary regarding compliance. The AA, ACIO, 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.

5.2 References

- DOC ITSPP section 4.4 (January 2009)
- Commerce Interim Technical Requirement 019, *Risk Management Framework (RMF)* (July 2012)
- NOAA *Continuous Monitoring Guidance for Annual Security Controls Assessments* (v4.0, February 2012)

6.1 NESDIS Security Controls Assessment Policy

As required by DOC ITSPP section 4.4.2, NESDIS system owners shall conduct an assessment of a subset of security controls in the information system at least annually or when a significant change occurs, whichever comes first, to determine the 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. In addition, in accordance with DOC ITSPP section 4.4.7, NESDIS system owners shall monitor the security controls in the information system on an ongoing basis.

The NESDIS-specific SCA process and procedures shall align with the practices prescribed in NIST SP 800-53A that are applicable for the system's assigned security categorization (i.e., High, Moderate, or Low). This document provides NESDIS-specific procedures for implementing the SCA process and should be used as companion document for implementation of NIST SP 800-53A within NESDIS and not as a replacement document.

NESDIS shall use the NOAA Security Controls Assessment Template located on the NESDIS IT Security Handbook web site at https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/it_security_handbook.php for documenting the SAP and for recording the assessment results at a summary level. It was prepared to fully comply with the NIST SP 800-53A assessment requirements.

The NESDIS ITSO shall monitor POA&M management by system owners and report status at least monthly to the NESDIS Assistant Administrator and Office Directors.

6.2 Policy Maintenance

The NESDIS ITSO shall review this policy and procedures 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 by e-mail to 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 AssessmentFundamentals

This section addresses the fundamentals associated with SCAs. The purpose of the SCA is to determine the 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. In order to successfully assess the control requirements, the SCA team must begin with the SSP Core Documents Package (see Section 9.0) and ensure appropriate techniques are utilized in performing the assessment of the controls documented in the SSP. Specifically addressed in this section are the assurance considerations, the different types of assessments, and the use of automated tools to increase the assurance in the security assessment.

7.2 System Security Plan

Security control assessments are performed against the control implementation as documented in the AO- (or AODR)-approved SSP Core Documents Package. (See NESDIS *System Security Plan Development and Maintenance Policy and Procedures* for additional details on the contents of a compliant SSP.) Therefore, an AO/AODR-approved SSP documenting all tailoring approved pursuant to Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*, must be in place prior to the start of the assessment for all types of security control assessments. A list of SSP Core Document artifacts that must be finalized before control assessment can begin are listed in Section 9.0.

7.3 Independence

Independence is defined in NIST SP 800-53 CA-4 Control Enhancement 1. Within NESDIS, SCAs of moderate and high impact systems must be performed by an assessment team that is independent from the SO. Low impact systems do not require independence unless required by the AO.

Independent SCAs performed for other types of security assessments (e.g., developer Security Test & Evaluation (ST&E), risk assessment, annual continuous monitoring, or POA&M closures) allow for the highest probability of reuse of the assessment results for SCA, which can reduce the overall cost of control assessments. The

NESDIS ITSO encourages the SO to utilize independent assessments for all control assessments whenever possible during continuous monitoring. If reuse of results is desired, the SO should coordinate with the Certifier to obtain agreement that the team has adequate independence prior to scheduling the assessment. The Certifier shall coordinate with the AODR regarding final approval of independence applicable to certification.

Table 1, *NESDIS Requirements for Independence*, documents the NESDIS requirements for independent testing based on the type of testing performed and the FIPS 199 impact level of the information system. For the annual SCA, independence is required for Moderate and High impact systems. Independence is also recommended for risk assessments at least annually, continuous monitoring where possible (e.g., use of NOAA Security Operations Center audit logging and reporting capabilities), and POA&M closures for Moderate and High impact systems.

Independence is optional for Low impact systems.

System Impact Level **Assessment Activity**	**Low**	**Moderate**	**High**
POA&M Closure Verification (Low Risk POA&Ms)	Optional	Optional	Recommended
POA&M Closure Verification (Moderate Risk POA&Ms)	Optional	Recommended	Recommended
POA&M Closure Verification (High Risk POA&Ms)	N/A	Recommended	Required
Risk Assessment	Optional	Recommended	Recommended during Continuous Monitoring, required for annual SCA
SCA	Optional	Required	Required
Continuous Monitoring (e.g., compliance/integrity and vulnerability scanning, audit logging)	Optional	Recommended	Recommended

Table 1 – NESDIS Requirements for Independence

7.4 Identifying Testing Targets

NIST 800-37 defines the purpose of a SCA is to “determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the system.” In order to meet this objective, the security control must be assessed on all components where it is applicable. The process of selecting an appropriate list of targets to assess is a delicate balance between assurance and cost of the assessment. Fully implementing CM-2 Configuration Baselines is the single largest factor in reducing the cost of control assessments. Properly implemented configuration baselines provide the justification for assessing a sample of the system's components rather than full examination of every component. Figure 1 describes the NESDIS process for selecting the target components for SCA examination and compliance testing.

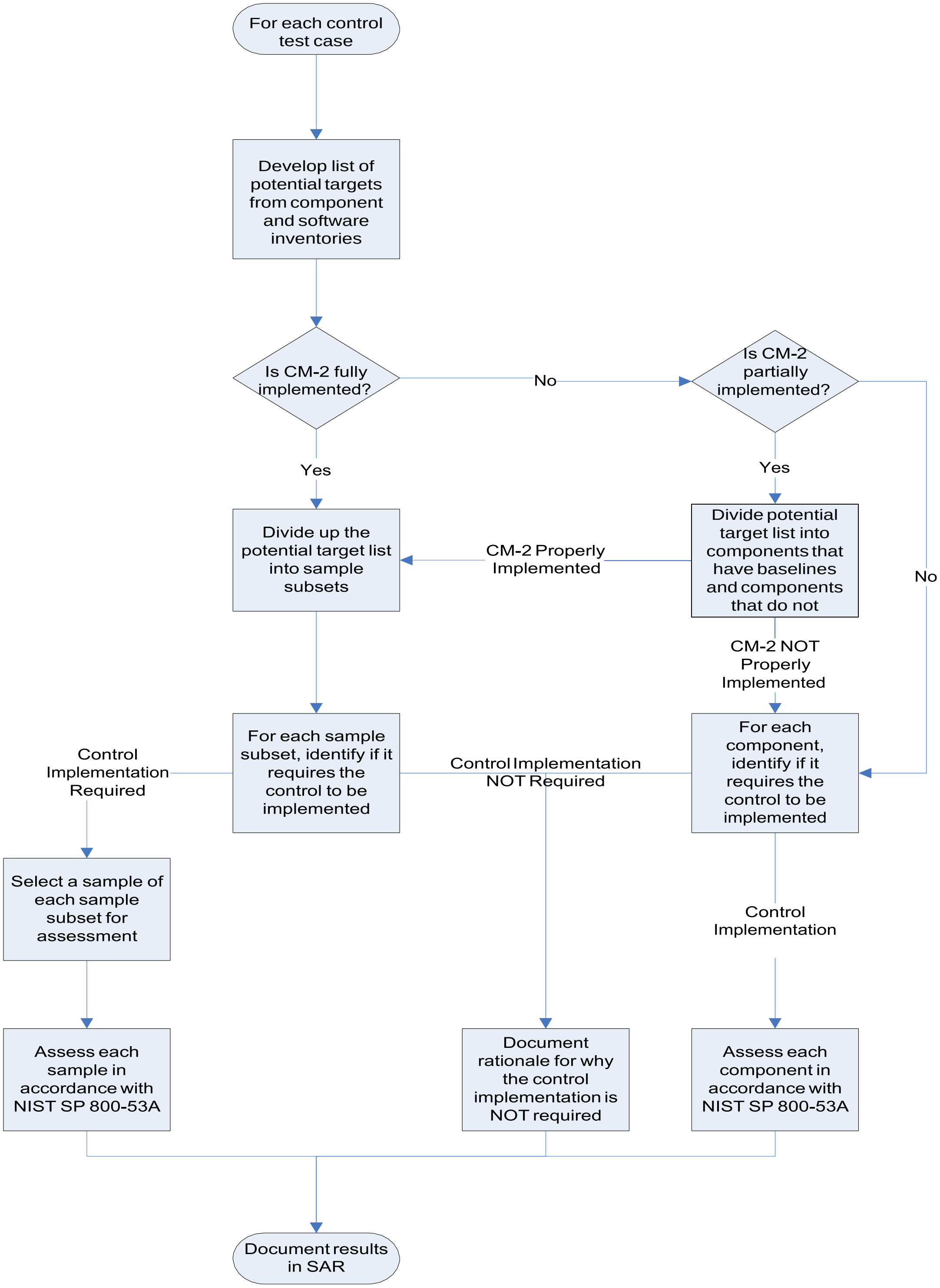
For each control test case
Develop list of potential targets from component and software inventories
Is CM-2 fully implemented?
No
Is CM-2 partially implemented?
Yes
Yes
No
Divide up the potential target list into sample subsets
CM-2 Properly Implemented
Divide potential target list into components that have baselines and components that do not
CM-2 NOT Properly Implemented
Control Implementation Required
For each sample subset, identify if it requires the control to be implemented
Control Implementation NOT Required
For each component, identify if it requires the control to be implemented
Select a sample of each sample subset for assessment
Control Implementation
Assess each sample in accordance with NIST SP 800-53A
Document rationale for why the control implementation is NOT required
Assess each component in accordance with NIST SP 800-53A
Document results in SAR

Figure 1 – Process for Determining Assessment Targets

7.4.1 Determine Assessment Targets

Determining the assessment targets begins with identifying the test case or security control being tested. Each test case requires the Certifier to re-evaluate the target list to ensure it is consistent with the assessment case. Once the Certifier identifies a target list, they may re-use that target list if the rationale for selecting the target list applies to other control tests.

7.4.2 Collect All Potential Targets

Selecting the assessment targets begins with the Certifier compiling a list of all possible targets. The list of potential targets is contained within the SSP Core Documents Package and/or the Quarterly Vulnerability Scan Package system inventories, both the component and the software inventories. Some technical controls require implementation at the application level and therefore need to be included in the potential target list[3].

7.4.3 Configuration Baselines

Once the list of potential targets is developed, the Certifier must determine if the configuration baselines exist for any or all of the targets identified. The Certifier should consider POA&Ms existing for remediation of CM-2 and CM-6 controls deficiencies to determine if the baselines are implemented properly, and therefore can be relied upon as described in the inventory. The Certifier can select a subset of the system components and software installations for assessment only if CM-2 and CM-6 are fully implemented. In some systems, CM-6 may be partially implemented (FDCC for Windows Workstations) and not implemented for others. In this case, the Certifier can use the baseline for the components that are configured to that baseline. Components that are not configured to a baseline need to be assessed separately, possibly manually, at 100 percent coverage.

7.4.4 Create Sampling Subsets

At this step, the Certifier can begin the process of creating sampling subsets ("buckets") of targets by configuration baseline. Each component must be placed into either a configuration baseline bucket or into a bucket indicating the component (or software installation) is not configured according to a baseline[4]. The SO must have sufficient documentation and testing to support placing a component within a

[3] For example, a web server will likely implement credentialed user logins. Controls from the AC and IA families in NIST SP 800-53 would apply and must be assessed.

[4] Each component must be configured according to the documented baseline in order to be placed within the baseline bucket. In some instances, the target may be initially configured to a baseline and then further modified in accordance with the configuration management process. The Certifier may determine if it is appropriate for the component to reside in the original configuration baseline bucket or be separated into a unique bucket based on the modified configuration. Special care should be taken when making this decision. The Certifier is highly encouraged to coordinate this decision with the ITSO to ensure it is acceptable for the SCA and authorization activities.

sampling subset[5]. Figure 2 depicts an example of dividing the component and software inventories into sampling subsets. The Certifier should be able to provide the rationale for placing any component or software installation into a sampling subset.

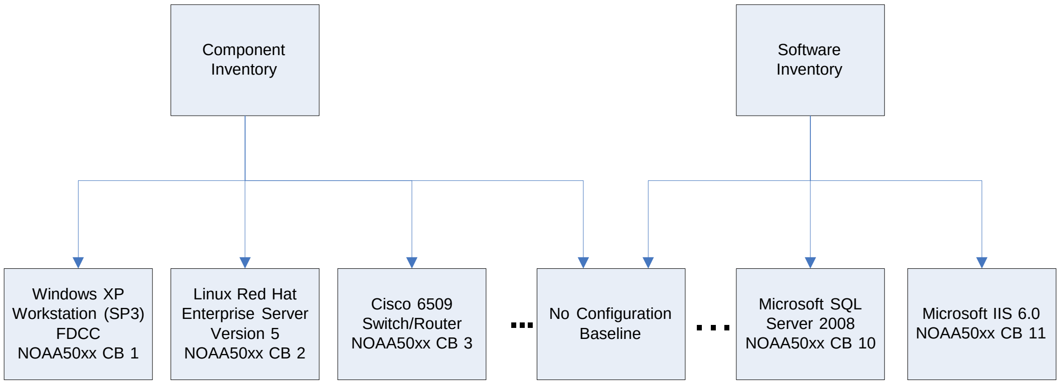
Component Inventory
Software Inventory
Windows XP Workstation (SP3) FDCC NOAA50xx CB 1
Linux Red Hat Enterprise Server Version 5 NOAA50xx CB 2
Cisco 6509 Switch/Router NOAA50xx CB 3
...
No Configuration Baseline
...
Microsoft SQL Server 2008 NOAA50xx CB 10
Microsoft IIS 6.0 NOAA50xx CB 11

Figure 2 – Example: Creating Sampling Subsets

7.4.5 Determine Control Implementation Applicability

Once the sampling subsets are created and every component and software installation is accounted for, the Certifier can begin the process of determining the targets to assess. In the context of the test case, the Certifier should evaluate the sampling subset to determine if the subset is required to implement the control. The Certifier should review the SSP and FIPS 200 to determine if the control is applicable[6]. If so, the sampling subset must be tested for the control. If not, the sampling subset can be eliminated from the test case. For the “No Configuration Baseline” subset, the Certifier must evaluate all individual components and software installations to determine if the control is required.

7.4.6 Select Samples

Once the sample subsets are identified, documented, and determined that the control must be implemented within the subset, the Certifier can select a representative and adequate sample from the subset that will be subjected to testing. The Certifier must provide the rationale behind the selection process. The Certifier can perform assessments on a random sample[7] within each sample subset. While the exact numbers of components to test per sample subset varies, NESDIS has provided guidance for determining an appropriate sample size in Table 2. The SCA team should collaborate with the Certifier to ensure the sample size identified is

[5] Some examples of sufficient documentation include configuration management records (e.g. CCRs), prior testing results, configuration files, and automated tool reports.

[6] The Certifer should utilize the SSP as a guide for determining if a control or test case is applicable. If the Certifier believes the control should be implemented in a baseline yet the SSP does not document its implementation, the Certifier should err on the side of caution and assess the control within that baseline and note the discrepancy with the SSP. The Certifier will make the final assessment of the control’s implementation.

[7] Certifiers may utilize the random number generator plug-in Data Analysis Tool available in the Microsoft Excel application, or equivalent, to generate the random numbers used for selecting items for sampling.

appropriate for the information system before testing begins. For components or software installation not configured in accordance with a configuration baseline, the SCA team must assess all components and software installations for the control. The use of automated configuration collection tools can significantly reduce the cost of assessing these components.

FIPS 199 Impact Level	Minimum Number of Components Sampled per Sample Subset	or	Minimum Percentage of Components per Sample Subset, whichever is greater
Low	5 if 5 or less total	or	If 6 or more total, 5 or 5%, whichever is greater
Moderate	10 if 10 or less total	or	If 11 or more total, 10 or 10%, whichever is greater
High	15 if 15 or less total	or	If 16 or more total, 15 or 25%, whichever is greater

Table 2 – NESDIS Guidance for Determining Sample Size per Configuration Baseline

7.5 Perform Assessment

Once the selection of targets is complete, the SCA team can begin the assessment of the controls on all the selected targets. More procedures for assessing the controls are documented in section 8.2.4.

7.6 Document Results

The Certifier is responsible for documenting all the results of the testing into the Security Assessment Report (SAR). In addition to the assessment results, the Certifier must document the rationale for creating sampling subsets and for NOT assessing components from a sample subset. Also, the Certifier must document the rationale for not assessing an individual component/software implementation when that component/software implementation is identified as not having a configuration baseline. The NESDIS ITSO is developing a *Security Assessment Report Policy and Procedure* for more details on the documentation requirements of the SAR.

7.7 Depth of Coverage

The FIPS 199 security impact level will determine the depth of testing required for the system. Depth of testing addresses the rigor and level of detail in the assessment. Low impact systems require a “generalized” assessment that “provides a level of understanding of the security control necessary for determining whether the control is implemented and free of obvious errors.” Moderate impact systems require “focused” assessment which “provides a level of understanding of the security control necessary for determining whether the control is implemented and free of obvious errors and whether there are increased grounds for confidence that the control is implemented correctly and operating as intended.” High impact systems require “detailed” assessment which “provides a level of understanding of the security control necessary for determining whether the control is implemented and free of obvious errors and whether there are further increased grounds for confidence that the control is implemented correctly and operating as intended on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control."

NOAA has developed a Continuous Monitoring/ Certification Test and Evaluation Template (located on the NESDIS IT Security Policy web page at https://intranet.nesdis.noaa.gov/ocio/it_security.php). This template implements the NIST SP800-53A test program specific for NESDIS. It includes within the test descriptions the type and level of testing to be applied to each impact level, and for each test objective. It also includes the expected test results for each test step and, when used to document the test results at a summary level, provides a standardized test report.

7.8 Assessment Types

There are four primary reasons for performing security control assessments: POA&M closure validation, control analysis as a part of the risk assessment, continuous monitoring, and security certification. Each of these has specific goals based on the purpose of the assessment. Below are short descriptions of each reason as well as unique requirements that impact the execution of the security control assessment.

7.8.1 POA&M Closure Validation

Security controls identified as deficient within the POA&M must be assessed before the POA&M can be closed. See the NESDIS *Plan of Action and Milestones Management Policy and Procedures* for additional guidance on managing POA&Ms.

POA&M closure does not require independent testing or oversight. However, independent testing would allow for the re-use of the testing for certification. NESDIS OCIO realizes it may be impractical to acquire independent services for the assessment of controls associated with POA&M closure requests. NESDIS OCIO will accept SO performed testing for POA&M closures; however, security control assessments not performed independently will not be used for certification.

7.8.2 Risk Assessment

As a part of the risk assessment, the SO must analyze the security control implementation as defined in the SSP for compliance with NIST SP 800-53.

NIST does not require independent testing performed during the control analysis phase of risk assessment. However, for FIPS 199 moderate and high impact systems, if the SO chooses to perform the control analysis using independent resources, the results may, with Certifier approval, be used for certification. Reuse of control analysis for certification can significantly reduce the overall cost of C&A. Therefore, the NESDIS OCIO recommends independent testing during the risk assessment process for Moderate and High impact systems.

7.8.3 Continuous Monitoring

The SO, or Common Control Provider, must develop a plan for continuous monitoring of selected controls after system deployment, and document the strategy in Appendix H of the SSP as well as reference the date, version, and title of the Plan in SSP section 16 under control CA-7. The Continuous Monitoring Plan should include an A&A Project Plan schedule that outlines the following activities and assigns responsibility to a specific role/position within the system and account for DOC, NOAA, and NESDIS policy requirements as well as any system-specific requirements for periodic controls monitoring, including but not limited to:

1. Quarterly vulnerability scanning (RA-5), including required scanning for unauthorized wireless access points for AC-18(2) as required by DOC ITSPP.
2. Semi-annual account reviews (AC-2).
3. Monthly Plan of Actions and Milestones (POA&M) updates (CA-5).
4. System maintenance (MA-2), including routine patching schedules (SI-2)
5. Annual SSP update (PL-2) including: review/update of the supporting documentation such as the PTA and PIA, if required (PL-5); continuous monitoring plan (CA-7); ETA and ERA, if required (IA-8); FIPS 199 analysis; FIPS 200 analysis; and system component inventory (CM-8).
6. Annual contingency plan (CP), business impact analysis (BIA), and CP test plan and results (CPTPR) updates; CP training, CP testing, and backup and recovery test (CP-2, CP-3, CP-4, and CP-9/CP-10).
7. Annual physical access record reviews (PE-2) and monthly visitor access record reviews (PE-8).
8. Semi-annual update of FISMA Inventory information in CSAM (PL-1).
9. Annual reviews of access agreements (PS-6 -- see DOC ITSPP, which requires agreements for people such as supervisors with access to PII – may not apply to all systems, depending on what the SSP requires for implementation of PS-6).
10. Annual risk assessment updates (RA-3), which would at a minimum coincide with scheduling of the annual independent security controls assessment for CA-2.
11. Semi-annual SI-7 integrity scans required by DOC ITSPP.
12. Annual role-based training of personnel with significant ITSec roles (AT-3), and professional certification (and certification renewal) of the ISSO as required by DOC CITR-006.
13. Annual incident response training (IR-2, IR-3).
14. Security Impact Analyses (CM-4) documented for all configuration changes, including supporting changes considered significant and any associated Interim Authorization to Test requests that require AO/co-AO approvals (CM-3, CA-6).
15. Monthly CyberScope reporting.

7.8.4 Annual Independent Security Controls Assessment

SCAs are the responsibility of the Certifier. Security assessment is the comprehensive evaluation of the management, operational, and technical security controls in an information system to determine the 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 (as documented in the approved FIPS 200 and SSP).

The SCA team may, at the Certifier's discretion, re-use the results of control assessments performed within the previous three years if testing was performed independent from the SO as described in NIST SP 800-53 control CA-2 and such assessment can be clearly demonstrated to not be impacted by changes to the system subsequent to the test. The Certifier must ensure that, over any given 3-year period, that 100 percent of the security control requirements have been independently assessed within the previous 3 years and the time since last assessment of any control, and the quality of the assessment, considered by the Certifier during the authorization recommendation process. The criteria for assessment reuse is detailed in NIST SP 800-53A, Revision 1, section 3.2.3.

7.9 Use of Automated Test Tools

Wherever feasible, automated tools should be utilized to collect data to support control testing. Using automated tools facilitates increasing both the coverage and depth of testing while reducing the expense to the SO. High impact information systems have the requirement to automate the maintenance of the baseline configurations. These automated mechanisms typically provide reporting functionality that can be used for the assessment of some security controls within the system.

In addition, the Security Content Automation Protocol (SCAP) is a method developed under the Information Security Automation Program (ISAP), a U.S. government multi-agency initiative for using standards to enable automated vulnerability management, measurement, and policy compliance evaluation to include FISMA compliance. These certified tools may generate results that satisfy the requirements for independence[8], resulting in significant cost savings. A description of the certification requirements can be found in the draft Security Content Automation Protocol (SCAP) Version 1.0 Validation Program Test Requirement9, which also contains pointers for locating the official list of certified products. When these tools are utilized properly, the need for sampling is greatly reduced.

[8] The Certifier may accept testing results from automated tools for analysis in the independent control assessments. SOs are encouraged to discuss the implementation of their SCAP complaint tools to increase the acceptance of the results for re-use in the SCA.

[9] Found at http://csrc.nist.gov/publications/drafts/nistir-7511/Draft-NISTIR-7511.pdf

8.1 NESDIS Security Controls Assessment Procedures

8.2 Preparation for the Assessment

Preparation for the SCA begins upon submission from the SO/ISSO of the SSP Core Documents package for compliance review (see Section 9.0). The time frame for this submission is 4 months prior to the target ATO date/ATO anniversary date. Upon receipt of the SSP Core Documents package for compliance review, the Certifier assigns the package components to the SCA team for a compliance review, and the team is provided 10 business days to complete the review and provide the completed SSP Compliance Review Checklist to the ISSO and SO. In addition, the Certifier begins the following planning activities that including initial development of the Rules of Engagement (ROE), Security Assessment Plan (SAP), A&A project plan schedule negotiation with the SO/ISSO, update of the SCA Continuous Monitoring controls distribution spreadsheet, and sampling of components in the system component inventory. The Certifier uses this preparation period to resolve schedule and inventory issues with the ISSO and SO before the SCA start date.

8.2.1 Rules of Engagement

The first task is for the Certifier and the SO/ISSO to come to an agreement on the Rules of Engagement (ROE) for the vulnerability assessment and/or penetration testing.

Topics to consider include the type of testing; tools used; level of access the SCA team will be granted while testing the system; scheduling issues for access to facilities, personnel, and the system; and the development and approval of formal procedures for accessing an operational system. This agreement must be written to include the level of access that will be granted as well as any restrictions on the SCA team.

In NESDIS, it is preferred for the vulnerability assessment team to analyze the scans performed by the ISSO and submitted for the quarterly scanning continuous monitoring requirement. The re-use of reports from automated continuous monitoring tools reduces the assessment time and examines the extent to which continuous monitoring requirements are effectively performed by the SO. If these submissions are used for the vulnerability assessment, then the Certifier does not need to document a separate ROE.

If the subject system is high-impact, then it requires internal and external penetration testing at least every 3 years. The Certifier first obtains copies of penetration test reports of the system dated within the last 2 years to determine from the scope if both internal and external testing have already been performed. If not, an ROE is needed to document the terms of the triennial penetration test.

8.2.2 Develop Security Assessment Plan (SAP)

After agreeing to the ROE terms, the Certifier develops the Security Assessment Plan (SAP) by reviewing the FIPS 200 approval and the SSP. The SAP provides detailed scope and procedures for the SCA team to perform the assessment, and references the ROE as a separate document if applicable. The SAP shall include sufficient detail to permit full, comprehensive testing by an entry-level assessor. The SAP is also incorporated into the Scope and Methodology discussion in the SAR, and variances between the SAP and the final executed SCA must be articulated in the SAR. The SAP also references the schedule for the SCA and Authorization Tasks of the annual A&A Project Plan as well as the controls selection for the SCA as documented in the Continuous Monitoring SCA Controls Distribution spreadsheet. Templates for the A&A Project Plan and the 3-year distribution for the SCA Continuous Monitoring controls selection are available on the NESDIS IT Security Handbook web site at https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/it_security_handbook.php, and details for planning activities are described in the *NESDIS Continuous Monitoring Planning Policy and Procedures*. The SAP shall describe the following for the SCA:

- Introduction/Purpose of the SCA (i.e., system ID, policy drivers, type of SCA such as annual or ATO renewal)

- Scope: the system's security categorization level, the FIPS 200 controls requirements baseline, and the version and date of the approved SSP Core Documents Package being tested.

- Approach/Methodology: the NIST, DOC, NOAA, and NESDIS policies and procedures to be followed for the SCA, as well as sampling requirements, Depth and Coverage, etc.

- Controls Selection Process: the criteria for reuse of prior assessments and criteria for controls selection for the current SCA as well as the list of controls selected as reflected in the SCA Continuous Monitoring Plan for the current year (updated by the Certifier as required based on the control selection criteria).

- SCA Team: Names, roles and contact information for personnel comprising the SCA team, including the Certifier, and description of the team's independence from the SO.

- System POCs: Key personnel with whom the SCA team will interact during the SCA including their roles and contact information.

- SCA Team Requirements: personnel, documentation, and component access requirements of the SCA team for conduct of the SCA, including lists of automated tools to be used, previous assessment reports to be reused, etc.

- SCA Schedule: Schedule for the SCA and authorization/re-authorization activities extracted from the A&A Project Plan for the current year's A&A/Continuous Monitoring activities.

8.2.2.1 Identify Controls to Test

8.2.2.1.1 Scope the Baseline

As the SCA team reviews the control implementation descriptions in the SSP, they should tailor the SCA Report spreadsheet to reflect the controls required in the system's baseline as well as which were selected for SCA. Every control and enhancement and their accompanying procedures that are determined applicable to the current system security baseline (after FIPS 200 required tailoring of NIST SP 800-53 controls) shall be checked in the applicability fields for the system impact level and the SCA year.

Controls and procedures not applicable to the system's impact level or current SCA year are not checked but remain in the spreadsheet. For each assessment procedure that is not required in the system's baseline (i.e., tailored out in the FIPS 200), reference, in the Expected Result column for the procedures, the version and date of the AO-approved FIPS 200 tailoring document. Additional guidance on control tailoring is provided in the NESDIS *FIPS 200 Security Control Selection and Tailoring Policy and Procedures*.

The assessment procedures for all requirements in the system's baseline must be accounted for as either assessed, tailored out, or that prior-year assessment results were reused. The procedures must be traceable back to the assessment objectives of the original control to permit a full mapping of what objectives are satisfied by the compensating controls, and which objectives are not addressed and will require an explicit risk acceptance by the AO. This will facilitate higher-level review of the results and help to ensure that the baseline controls have been appropriately addressed.

Some controls not fully implemented per the SSP may be documented by referencing the POA&M established to implement the control requirement. Controls associated with existing POA&M deficiencies do not need to be re-assessed by the SCA team until the POA&M is closed. The test team can mark that control as Other than Satisfied in the Results without performing the control assessment procedures, referencing the POA&M number in the appropriate column of the spreadsheet. While the assessment procedures do not need to be performed, the control is still applicable for the system and is still required and accounted for in the SCA results reported in the SAR. The portion of a control that is partially implemented must be assessed and documented to give the AO a more accurate assessment of the risk to operate the system.

8.2.2.1.2 Identify Compensating and Supplemental Controls

Where the SO has indicated a control is implemented through a compensating control or a supplementing control has been added to the baseline, the Certifier needs to develop new assessment cases to verify the new control. These assessment cases shall be developed to provide assurance appropriate for the system's impact level. If the compensating control is not within the 800-53 control catalog, close coordination with the ITSO/Certifier is essential to ensure that the control is fully assessed.

8.2.2.1.3 Common Controls

Common controls can simply be marked as being satisfied through common controls; however, they still require at least a basic assessment. Any control in the SAP identified as being a common control or the system's responsibility of a hybrid control must be assessed in accordance with the NIST SP 800-53A procedures. If the SCA team examination of the SSP control implementation finds inheritance of a common control but finds that the control is not demonstrably implemented as common by the system or its environment, then the common control cannot be used and the control must be assessed at the appropriate impact level. SOs are responsible for ensuring that common controls applicable to and inherited by their information system are fully implemented to meet the system's requirements. The SCA team shall work in close cooperation with the Certifier to fill any gaps in the assessment of the common controls implementation when the common control is supplemented by the system or when the control is inadequately tested for the system's impact level. For examples:

- If the SSP specifies inheritance of the NOAA hybrid control for RA-5, which requires that the NOAA-mandated scanner is used for vulnerability scanning, but the system does not use the NOAA-mandated scanner, then the SCA team evaluates the scanner in use as to its performance and compliance with all RA-5 requirements specific to the scanning tool.
- If the system inherits a Common Control that is Other than Satisfied and the CCP is tracking a POA&M for remediation, the SO may opt to implement mitigating system-level safeguards until the CCP remediates the POA&M. In this instance, the SCA team will assess the mitigating controls and take the results into consideration for the overall control status.
- Common controls implemented and tested at the Moderate baseline may not have implemented the additional requirements for a high impact system. Therefore, the SO for a High impact system may choose to supplement the common controls to address the delta requirements between Moderate and High, and the SCA team would assess the supplemental controls. See the NESDIS *Security Control Selection and Tailoring Policy and Procedures* for additional guidance on the use of common controls.

Finally, where current testing results are available and with Certifier concurrence, those results can be used. In this case, document the source and result in the SCA Report spreadsheet; however, the assessment procedures do not have to be redone.

8.1.3 Control Selection Criteria

- Annual Required: 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). The SCA Continuous Monitoring Plan spreadsheet 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.

- Closed POA&Ms: 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 remediated by a POA&M closed in the year preceding the date of SCA start.
- Annual Selected/3-year: 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.
- Other criteria: Incidents that resulted in system compromise due to control failure, new controls added to the baseline (as happens upon issuance of new revision to SP 800-53), and controls pertaining to AO/ITSO/SO/ISSO specific requests or concerns.

8.1.4 Select Assessment Methods

The Certifier must provide anticipated results for each assessment case to align with security control implementations as described in the SSP and applicable Common Control documents. After the specific assessment test step modifications have been identified in the template, assessment methods and objects must be selected to appropriately verify the implementation of the control for every type of "component" as modified for sampling. With these methods identified and modified, the anticipated results must be documented prior to Certifier approval of the test plan. Where the standard template is modified, the modifications must be consistent with SP 800-53A as interpreted by the Certifier.

8.1.4.1 Finalize Assessment Procedures

Once the controls to be assessed and assessment methods have been identified, the Certifier develops assessment procedures for each control. Assessors should supplement the assessment procedures in the NESDIS template as necessary to fully assess the system. Specific assessment procedures or guides should be developed for each assessment method. The procedures may be further organized and possibly divided into separate documents to help focus the assessor on the specific controls and objects under consideration.

8.1.4.1.1 Document Review

Documents required for examination should be identified in the test plan and the list should be verified and updated. As each control is evaluated while the assessment plan is being developed, the document expected to address the control should be specified with that control, or the general topic expected to address the control should be provided if a specific document cannot be identified. The updated document list should be delivered to the ISSO no later than with the final plan, one week prior to the start of the actual execution of test procedures. Documentation includes any document, procedure, or plans referenced in the SSP. System audit log files and firewall logs may be provided for verification of periodic monitoring analysis, but system testers will still be required to collect fresh copies of the logs to ensure that the control is operating as expected by verifying records of test activities. The ISSO shall maintain all documentation referenced in the SSP in a binder or virtual binder (e.g. file system with a folder for each control, or a ‘wiki’) to support control testing as well as to provide a central library of all security relevant documentation for the system.

8.1.4.1.2 Interview

The Certifer shall also develop interview questions for all interviews. Personnel from all levels of the organization should be interviewed, from the SO, through the ISSO and system personnel, including user representatives. Facilities managers should also be interviewed where appropriate. Higher impact level systems require more interviews and a wider range of roles than required for low impact levels. Interview questions should be appropriately grouped for the level and expected knowledge of the interviewee. For example, the SO should not be questioned about specific configuration settings, while system administrators should not be questioned about system funding priorities. Interview procedures should include an expected duration for the interview to assist the ISSO in scheduling personnel for the interview.

8.1.4.1.3 Examination

A list of observation items shall also be developed for Assessment team personnel to look for whenever they are at system locations. All locations containing system components including alternate sites shall be assessed for Operational and Management controls. Observations should not be limited to a specific time identified as the observation period, but time must be scheduled to walk through system spaces to observe physical and environmental controls and adherence to operational procedures. The Assessment team should observe adherence to procedures throughout the test period, such as whether the Assessment team is subjected to applicable visitor controls, or whether system administration personnel adhere to Access Controls such as password length.

8.1.4.1.4 Technical Testing

The Certifier shall identify the specific settings to examine or commands to execute to assess the applicable control implementations for each "bucket" identified in section

7.2.2.4 of this document. For each setting or command, the Certifier shall supply acceptable values for settings and expected results of the commands. These procedures will be reevaluated prior to execution to incorporate findings from document reviews and interviews. The Certifier shall coordinate with the ISSO during a 30-day period prior to the start of the SCA to ensure that the SCA team can obtain a random sample of components for testing from the component inventory provided in the SSP Core Documents package for compliance review.

8.1.5 ISSO review and Certifier Approval

After the SAP has been developed by the Certifier, it shall be submitted to the ISSO for ISSO/SO review and approval within 3 business days of the start date of the SCA. The ISSO and SO shall review the SAP and submit any comments or concerns back to the Certifier within two days. Significant issues should be raised with the Certifier as soon as they are identified to minimize the chance of test plan revisions delaying the schedule start of testing. The Certifier will update the SAP as necessary to address any issues raised by the ISSO and SO and route the final SAP within one business day for final signatures.

8.1.6 Schedule Assessment Execution

After the assessment plan has been developed, it needs to be properly executed to provide the needed level of assurance. The ISSO shall finalize the schedule of resources necessary to support test execution when the test plan is delivered. The ISSO shall coordinate with the SO, systems personnel, representative users, and any other personnel with responsibility for any aspect of system security to schedule interviews for the first week of test execution. The ISSO shall also work with the system and network administrators to identify personnel with appropriate expertise and access permission required to execute the assessment plan. The ISSO should consider scheduled training, vacations, and organizationally mandated events when selecting personnel. The ISSO shall also ensure that formal procedures have been developed and approved if required for access to an operational system.

System personnel shall review all technical assessment procedures as they are being performed to ensure that no actions are taken that may harm an operational system[10]. The ISSO will also work with system and network administrators to schedule times for to perform the test that do not interfere with operational restrictions. Scheduling must include considerations for operational necessities. Operational circumstances that would prevent testing should be considered and avoided, and contingency scheduling

[10] The SO, ISSO, and system administrators may decide to stop a test if it may cause an operational disruption. However, the SO should note that the Certifier will likely identify the control as not fully met if the test was not properly performed. A residual risk will be documented in the SAR. SO are encouraged to work with the testing team to find alternate ways of evaluating the control's implementation to ensure a complete test is performed.

should be included if the system is prone to unanticipated high-priority events that could bump scheduled test activities.

8.2 Assessment Performance

Assessment methods are identified in NIST SP 800-53A. The NESDIS implementation of that process for actually assessing the security controls is shown in Figure 2: Control Assessment Sequence.

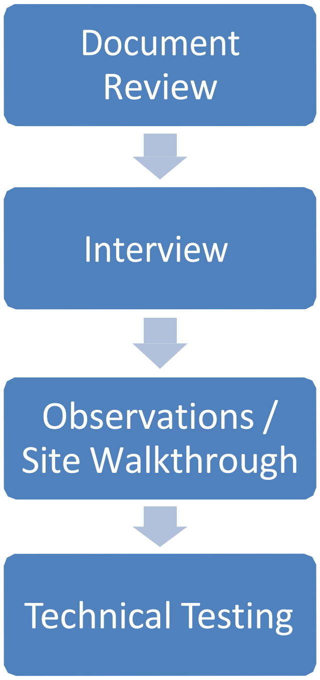

Figure 3 – Control Assessment Sequence

8.2.1 Documentation Review

Assessment execution will begin with documentation review. Review of documentation provided in support of the SSP can begin as soon as the SCA receives the documents from the SO. Documentation reviews do not need to occur on site and can occur prior to the technical or on-site test and at any location authorized to store any sensitive material contained in the documents. Test results from document examinations need to cite the document and page of the data that appropriately provides the information to satisfy the test, as well as either copy or paraphrase the material into the test report. Since the purpose of security control assessment is to verify implementation of controls documented in the SSP, the SSP cannot be a source document to verify a control implementation. If the provided documents do not fully address the controls, the SCA should request additional documentation or clarification as required.

8.2.2 Interview

Upon arrival on site, the SCA will begin interviewing personnel. It is insufficient to interview only the ISSO to confirm security control implementations. System and network administrators, as well as a representative sample of users that reflect the major functions of the system, should be interviewed. Interviews may be conducted by two SCA members to help ensure that the assessor correctly interprets interview responses.

While assessors should follow the documented procedures as closely as possible, they are encouraged to pursue impromptu questions if a response reveals unanticipated information that opens the line of questioning. Interview subjects should be identified by their position or role in the system. Wherever possible, multiple personnel for each position or role should be interviewed to determine if there is consistency in descriptions of the operational environment and to permit some degree of anonymity when reporting the results. Interview responses should be consolidated as much as possible, and not linked to a specific person in the final report. Personnel can be reluctant to report negative information if they know the disclosure will be linked directly to them personally. Artifacts from interviews should include the interview procedures and, at a minimum, the interviewer's summary of the answer. The interview results should factually document the interview subject's perception of the control implementation and not attempt to determine the acceptability of risks resulting from the implementation. For example, interview results should be "subject stated that the implemented control setting is xxxx", not "subject stated that the control implementation is sufficiently strong for system yyyy".

Results must be aggregated and transferred to the control assessment report template prior to the start of technical testing to permit adjustments to the technical procedures.

8.2.3 Site Walk-through

A site walk-through should also be performed early in the test process to minimize the interference and optimize the use of assessment time. The walk-through is the opportunity to observe physical and environmental controls, locations of printers, monitor positions, physical access controls, and general adherence to documented procedures. During the walk-through, testers should not voluntarily perform procedural controls (unless directed to do so by local personnel) (e.g. tester should attempt tailgating through controlled portals rather than using an assigned badge, or attempt to enter while not signing visitor logs, etc.) to determine how seriously personnel treat procedural controls judge the reaction of system personnel to procedural violations.

However, the SCA should remember that this is not a penetration test and should only be used as an opportunity to observe physical controls and adherence to procedures.

The SCA should keep the observations list and report form with them at all times to note discrepancies noticed whenever they are within system facilities or while other tests are performed.

8.2.4 Technical Test

Prior to beginning technical testing, interview results should be reviewed for results that conflict with the control implementations documented in the SSP, which may require adjustments to the assessment cases. Such reviews should occur at least two days before technical testing is scheduled to occur to permit updating the procedures. The original and updated assessment cases should then be available for technical testing in case the data gathered during interviews is incorrect. Specific components for sampling may also be randomly selected from the subsets of components based on the sampling requirements. See section 7.2.2.6 for guidance on setting up the sampling subsets.

Configuration Management controls, specifically CM-2 and CM-6, should be assessed early in the assessment process, and the results leveraged to select test samples to reduce the amount of technical testing required as described in section 7.2.2.6.

At either party's discretion, the independent assessors can perform technical testing, or they can direct system personnel to perform the procedures under the direct guidance of the assessors if the SO is reluctant to permit them direct access to the system.

Technical assessments shall consist of an assessor who will perform the procedure or assist the system or network administrator in following the procedures and a second assessor with a copy of the procedures to document the results of each step. Successful completion of each procedure may be documented through screen captures, logging the session to a file, capturing specific details that would permit locating audit log records of the test activities, or free-hand documenting the observed results as long as sufficient information is provided to convey the results to an independent auditor. While the specific technique for documenting an assessment will vary depending on the specific control, the recommended impact level for which it would be appropriate to utilize a technique is documented in Table 3.

Documentation Technique	Impact Level
Screen Captures	High
Log Session to File	High
Capture specific details in digital form to permit locating records of the test activities	Moderate
Free-hand documenting the observed results	Low

Table 3 – Recommended Impact Level for documentation techniques

Assessment results must contain sufficient detail to provide assurance to an independent reviewer that the procedure had been performed and can be sufficiently duplicated by rerunning the test procedures. Therefore, detailed sensitive information may be collected in the course of the assessment. After assessment procedures have been executed, the SCA should collect all supporting artifacts that verify that events are appropriately captured in the audit logs. All artifacts must be marked "For Official Use Only" and submitted with the assessment report.

The time required to perform technical testing depends on many variables, including the number of subsets of components (sample groups), the number of components to assess, the degree to which automated mechanisms can be utilized to collect configuration data, and the expertise of personnel involved in performing the assessment. After all procedures have been performed, the SCA should provide a summary out-briefing to the SO to present the overall impression gained from the testing and provide any preliminary results that may be available. This is an informal presentation intended to provide overall impressions and significant discrepancies observed during assessment performance. The SCA should refrain from providing any definitive statement about the results of the assessment until they have had time to fully analyze the results. Instead they should comment on the verified observations that will provide the basis for the conclusions and recommendations.

8.3 Output Requirements

After all planned assessment steps have been performed, the Certifer must generate a Security Assessment Report (SAR) that documents the results of the assessment. The assessment results documented in the report are the factual observations of *effectiveness* for each instance of control implementation based on the assessment performed. The assessment results are not an evaluation of the *adequacy* of the control or its implementation since that judgment is the responsibility of the AO as part of the FIPS 200 and SSP development controls baseline determination and documentation activities. The assessment report must provide sufficient detail to provide assurance to an independent auditor that the assessment has been performed and the result is accurately described, must summarize the overall results for each control, and must identify deficiencies and corrective actions. The AO is then briefed on the assessment results and approves POA&Ms.

8.3.1 Security Assessment Report

Within NESDIS, SCAs must be documented using the NOAA Continuous Monitoring/Security Controls Assessment (SCA) Report Template and companion guidance located on the NESDIS IT Security Policy web page at https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/it_security_handbook.php, and the vulnerability scan analysis is reported in the Vulnerability Assessment Report (VAR).[11] The reporting form includes all required elements—the NIST SP 800-53 list of controls; an area for documenting the continuous monitoring plan of controls required and selected for assessment in years 1, 2, and 3 of the authorization cycle for SCA; the assessment objectives and methods; assessment steps, evidence, and results—and can be customized for systems of all impact levels (high, moderate, or low). The Certifier shall document their recommendations for correcting all deficiencies identified

[11] See the NESDIS *Policy and Procedures for Conducting Security Controls Assessments* for more information.

or shall reference the CSAM POA&M number where corrective actions are documented.

Each assessment step performed must have an associated conclusion (see drop-down menu choices in the template) with results explained in sufficient detail that an independent reviewer would reach the same conclusion after reviewing the artifacts listed as evidence. The final assessment of the control's implementation status is made by the Certifier if it is an SCA. All failures identified during control assessments that the SO cannot immediately correct must be mapped to one of two dispositions—either it is documented in a POA&M[12] if remediation is possible, or documented in a revision to the FIPS 200 as controls baseline tailoring[13] if remediation is not possible or is not cost-effective security—and then approved by the AO.

The Certifier uses information from the SSP, the Security Assessment Plan, the SCA Report spreadsheet, and the VAR results to update the Risk Assessment Report (RAR).[14] The RAR is then uploaded to CSAM.

The Certifier next uses information from the SSP, SAP, and RAR to update the Security Assessment Report (SAR).[15] The SAR is then uploaded to CSAM and is used as the basis for the Certifier's Recommendation memo from the Certifier to the SO upon conclusion of the SCA, and as the basis for the Briefing to the AO/co-AOs (see section 8.3.2.).

The Certifier shall upload to CSAM all artifacts collected during the assessment execution along with the final Security Assessment Report. Assessment reports, findings, and artifacts shall be treated as sensitive data, marked "For Official Use Only," and handled in accordance with Commerce and NOAA policies for handling sensitive information.

8.3.2 Briefing the AO

The SO must brief the AO (or co-AOs) on the results of annual assessments, and the Certifier must assist the SO in briefing the AO (or co-AOs) on the results of SCA, at which time AO/co-AO approval of risk, all POA&Ms, and any FIPS 200 revisions are obtained. Annually, the AO/co-AOs must approve all POA&Ms from the SCA, and acknowledge that the AO/co-AOs continue to accept the residual risk of operating the system.

8.3.3 Submission

The assessment report with all supporting artifacts must be submitted to the NESDIS ITSO as follows:

[12] See the NESDIS *Plan of Action and Milestones Management Policy and Procedures* for more information.

[13] See the NESDIS *FIPS 200 Security Control Selection and Tailoring Policy and Procedures* for more information.

[14] See the NESDIS *Policy and Procedures for IT Security Risk Management and Conducting Risk Assessments* for more information.

[15] See the NESDIS *Security Assessment Report Policy and Procedures* for more information.

- For certification assessments, the assessment team submits the assessment report and supporting artifacts via encrypted email or hand-delivered on CD to the NESDIS ITSO/Certifier no less than 60 calendar days prior to the target authorization date (see the NESDIS *Risk Management Framework Assessment and Authorization Process Policy and Procedures* for more information).
- For annual controls assessments, the SO submits the assessment report and supporting artifacts via encrypted email to the NESDIS ITSO/Certifier no less than 11 months from the accreditation date for the Year 1 assessment or anniversary of the accreditation date for Years 2 and 3 (see the NESDIS *Continuous Monitoring Planning Policy and Procedures* for more information).
- For POA&M closures, the SO or ISSO uploads the assessment report and supporting artifacts to the “artifacts” section of the POA&M in the CSAM system (see the NESDIS *Plan of Action and Milestones Management Policy and Procedures* for more information).

9.0 SSP Core Documents Package

The contents of the SSP Core Documents package are listed below. All documents must be in the latest template and latest NIST version requirements and uploaded to the system's CSAM Status page as SSP artifacts.

- SSP with Appendices [not yet signed by AODR for Compliance Review submission, but must be AODR-approved for SCA start]
- Apx A: FIPS 199 Security Categorization [final, signed by AO/co-AOs]
- Apx B: LO & Personnel Lists
- Apx C: System Description
- Apx D: System Environment & Component Inventory
- Apx E: Related Laws/Regulations/Policies (including system-specific policies and procedures referenced in the SSP control implementation descriptions)
- Apx F: Rules of Behavior
- Apx G: Privacy Threshold Analysis [final with Signatures] and Privacy Impact Analysis (if required) [accepted by NOAA Privacy Officer]
- Apx H: Continuous Monitoring Plan (controls distribution spreadsheet) and A&A project plan (see template on the NESDIS IT Security Handbook website)
- Apx I: Interconnection Security Agreements (MOU, MOA, ISA, SLA) [finals, with Signatures]
- Apx J: Contingency Plan [final, with Signatures] and Business Impact Analysis
- Apx K: Contingency Plan Test Plan & Results
- Apx L: Risk Assessment Report
- Apx M: Designation Letters (AO, SO, ISSO, ATO, IATT) [signed]
- Apx N: FIPS 200 Analysis [final, signed by AO/co-AOs]
- etc. : Other system-specific Appendices added by the system owner such as Standard Operating Procedures or AO-approved (via the FIPS 200) Scan Exclusion Lists.
- E-Authentication Threshold Analysis [with SO Signature]

- E-Authentication Risk Assessment (if required)
- Configuration Management Plan (referenced in CM-9)
- Incident Response Plan (referenced in IR-8)

The package cannot be accepted for compliance review or for SCA start without filnal/approved requirements baseline as documented in the FIPS 199 (Appendix A) and FIPS 200 (Appendix N). The SSP and the supporting documents describe how this baseline is implemented for the system, so if the baseline is not AO/co-AO approved, the implementation has no foundation.

The hierarchy of requirements is as follows:

- Level 1: U.S. Public Laws (such as FISMA), Federal policies (such as OMB mandates), directives (such as Executive Orders, Homeland Security Presidential Directives, and Federal Information Processing Standards), federal implementation procedures in the NIST Special Publication series, and Agency policy (such as the DOC ITSPP and NOAA IT Security Policy).
- Level 2: Security controls baseline documents that define which of the Level 1 requirements are applicable to the system – the FIPS 199 analysis sets the foundation for the baseline level of high, moderate, or low, and the FIPS 200 analysis reflects how the minimum recommended control requirements apply to the system.
- Level 3: The SSP and supporting Core Documents describe how the Level 2 requirements baseline control objectives are met for the system, including tracking of POA&Ms in instances where the Level 2 control objective requirement is not fully met.

Approval Page

Document Number: NQP-3410, Revision 2.1	
Document Title Block: **Policy and Procedures for Conducting Security Controls Assessment**	
Process Owner: NESDIS Chief Information Division	Document Release Date: May 15, 2013

Prepared by:

Erica Boyd 3/26/15
Erica Boyd Date:
Ambit- Associate Consultant
NESDIS Chief Information Office

Approved by:

Irene Parker 3/26/15
Irene Parker Date:
Assistant Chief Information Officer - Satellites

Document Change Record

VERSION	DATE	CCR #	SECTIONS AFFECTED	DESCRIPTION
2.1	**March 26, 2015**	**----**	**ALL**	**Baseline NQP-3410**