

**Non-Exchange Entity (NEE) Information Security  
and Privacy Continuous Monitoring (ISCM)  
Strategy Guide**

**Version 1.1**

**July 29, 2019**

## Executive Summary

The Centers for Medicare & Medicaid Services (CMS) is responsible for implementing many provisions of the Patient Protection and Affordable Care Act of 2010 (hereafter referred to as the “Affordable Care Act” or “ACA”). Protecting and ensuring the confidentiality, integrity, and availability (CIA) of the Health Insurance Exchange (hereafter simply the “Exchange”) information, common enrollment information, and associated information systems is the responsibility of the Exchange and all its business partners. CMS is responsible for providing business, information, and technical guidance; creating common baselines and standards for information technology (IT) system implementation activities; and maintaining oversight of the CMS Federally-facilitated Exchange (FFE) and IT systems that support the Exchange and common enrollment IT systems. FFE partners are considered Non-Exchange Entities (NEE)<sup>1</sup> and, as such, are required to comply with the privacy and security standards that are at least as protective as the standards the Exchange has established and implemented for itself.<sup>2</sup>

Information security and privacy continuous monitoring (ISCM) is a dynamic process that must be effectively and proactively managed to support organizational risk management decisions. ISCM provides a mechanism for the NEE organization to identify and respond to new vulnerabilities, evolving threats, and a constantly changing enterprise architecture and operational environment, which can feature changes in hardware or software, as well as risks from the creation, collection, disclosure, access, maintenance, storage, and use of data. Through ongoing assessment and authorization, CMS can detect changes to the security and privacy posture of a NEE IT system, which is essential to making well-informed, risk-based decisions about the system within the CMS environment.

This ISCM Strategy Guide describes CMS’s strategy for instructing NEEs in following the initial approval of the Request to Connect (RTC) to the CMS Data Services Hub. This guide conveys the minimum requirements for NEEs that implement an ISCM program for their systems and maintain ongoing CMS RTC approval to receive eligibility determination and enrollment data services from the CMS FFE. The ISCM activities begin as soon as the RTC has been approved.

## About This Document

This document provides guidance on the necessary ISCM process and ongoing authorization for maintaining a security and privacy risk posture that meets CMS requirements.

This document uses the term *authorizing official* (AO), which refers to the NEE’s Authorized Official or Chief Information Security Officer / Senior Officer of Privacy

---

<sup>1</sup> 45 CFR § 155.260 (b)(1)

<sup>2</sup> NEEs are required to comply with the privacy and security standards consistent with 45 CFR § 155.260(a)(1) - (6), including being at least as protective as the standards the Exchange has established and implemented for itself under 45 CFR § 155.260(a)(3).

(equivalent) who signed the Interconnection Security Agreement (ISA).

The term *authorization* refers to the CMS Approval of the Request to Connect via the ISA.

The term *Independent Third-Party Assessor* (Auditor) is defined as an Auditor that is independent with no perceived or actual conflict of interest involving the developmental, operational, and/or management chain associated with the system and the determination of security and privacy control effectiveness. The Auditor must be free from any real or perceived conflicts of interest, including being free from personal, external, and organizational impairments to independence, or the appearance of such impairments to independence.

## Who Should Use This Document?

CMS intends this document for use by NEEs associated with the FFE, auditors, government employees and contractors working on ACA projects, and staff supporting the CMS organization.

## How This Document Is Organized

This document consists of three sections and three appendices:

- Section 1 provides an overview of the continuous monitoring process.
- Section 2 describes roles and responsibilities for stakeholders other than the NEE.
- Section 3 describes how operational visibility, change control, and incident response support continuous monitoring.
- Section 4 summarizes the CMS reporting requirements and internal NEE activities.
- Appendix A describes the monthly and quarterly reporting summaries.
- Appendix B describes the security and privacy controls action frequencies.
- Appendix C describes the subset of security and privacy controls that must be tested annually.

## How to Contact Us

Please direct all questions about this document to [directenrollment@cms.hhs.gov](mailto:directenrollment@cms.hhs.gov).

## Table of Contents

|                                                                             |           |
|-----------------------------------------------------------------------------|-----------|
| <b>1. Overview .....</b>                                                    | <b>1</b>  |
| 1.1 Purpose .....                                                           | 1         |
| 1.2 Continuous Monitoring .....                                             | 1         |
| <b>2. Continuous Monitoring Roles and Responsibilities .....</b>            | <b>3</b>  |
| 2.1 NEE Organizational Authorizing Official .....                           | 3         |
| 2.2 CMS Chief Information Security Officer .....                            | 3         |
| 2.3 CCIIO Information System Security Officer .....                         | 3         |
| 2.4 Third-Party Independent Assessor Organization (Auditor) .....           | 4         |
| <b>3. Continuous Monitoring Process Areas .....</b>                         | <b>4</b>  |
| 3.1 Operational Visibility .....                                            | 4         |
| 3.2 Change Control .....                                                    | 5         |
| 3.3 Incident Response .....                                                 | 7         |
| <b>4. Continuous Monitoring Reporting Requirements .....</b>                | <b>8</b>  |
| <b>Appendix A. Continuous Monitoring Reporting Summary .....</b>            | <b>9</b>  |
| <b>Appendix B. Control Action Frequencies .....</b>                         | <b>10</b> |
| <b>Appendix C. Annual Assessment of Security and Privacy Controls .....</b> | <b>18</b> |

## List of Figures

|                                                               |   |
|---------------------------------------------------------------|---|
| Figure 1. NIST SP 800-137 Continuous Monitoring Process ..... | 2 |
|---------------------------------------------------------------|---|

## List of Tables

|                                                                    |    |
|--------------------------------------------------------------------|----|
| Table 1. Control Selection Criteria .....                          | 5  |
| Table 2. Control Frequencies .....                                 | 11 |
| Table 3. Security and Privacy Controls to Be Tested Annually ..... | 18 |

# 1. Overview

The Centers for Medicare & Medicaid Services (CMS), through the Center for Consumer Information and Insurance Oversight (CCIIO), is responsible for providing business, information, and technical guidance; creating common baselines and standards for information technology (IT) system implementation activities; and maintaining oversight of the Federally-facilitated Exchange (FFE) and IT systems that support the Health Insurance Exchange (hereafter simply the “Exchange”) and common enrollment IT systems. FFE Partners are considered Non-Exchange Entities (NEE) and, accordingly, must comply with the privacy and security standards that are at least as protective as the standards the Exchange has established and implemented for itself.

Monitoring security and privacy controls is part of CMS’s overall risk management framework for information security. Within the CMS Risk Management Framework (RMF), authorization approval occurs through the Request to Connect (RTC) process. Once a NEE’s authorization is approved, the NEE’s security and privacy risk posture is monitored according to the ongoing assessment and authorization process. The NEE is required to maintain a security authorization that meets CMS requirements. Traditionally, this process has been referred to as “Continuous Monitoring” or “Ongoing Security Assessments.” Both terms are essentially synonymous and should be so interpreted.<sup>3</sup>

Performing ongoing security and privacy assessments determines whether the set of deployed security and privacy controls remain effective given the dynamic threat landscape and whether these controls provide adequate response to changes that may occur in the system and its environment over time. To maintain the information security and privacy risk posture of an IT system, the NEE must monitor and regularly assess its security and privacy controls. The ISCM activities begin as soon as the RTC has been approved.

## 1.1 Purpose

This document provides the NEEs with guidance and instructions on how to implement their own ISCM program. This document also addresses the deliverables and artifacts that the NEEs are required to deliver to CMS.

## 1.2 Continuous Monitoring

The CMS continuous monitoring program is based on the continuous monitoring process described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organization*. The goal of continuous monitoring is to provide (1) operational visibility, (2) managed change control, and (3) attention to executing incident response duties.

---

<sup>3</sup> Continuous Monitoring is described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*. Other NIST documents, such as NIST SP 800-37, Rev. 1, refer to “ongoing assessment of security controls.”

The support of the NEE's continuous monitoring capability facilitates ongoing authorization and reauthorization decisions. Security and privacy-related information collected during continuous monitoring is used to update the security authorization package. This information provides objective evidence that demonstrates the continued effective implementation of the CMS baseline security and privacy controls. Security status reporting provides NEE and CMS Authorizing Officials (AO) with the necessary information to make risk-based decisions and offers assurance to other relevant entities regarding the security posture of the IT system.

As defined by NIST, the process for continuous monitoring includes the following activities:

- **Define** a continuous monitoring strategy based on risk tolerance that maintains clear visibility into assets and awareness of vulnerabilities and utilizes up-to-date threat information.
- **Establish** measures, metrics, and status monitoring and control assessments frequencies that make known organizational security status; detect changes to information system infrastructure and environments of operation; and provide status of security control effectiveness to support continued operation within acceptable risk tolerances.
- **Implement** a continuous monitoring program to collect the data required for the defined measures; report on findings; and automate collection, analysis, and reporting of data where possible.
- **Analyze** the data gathered and **report** findings accompanied by recommendations. It may become necessary to collect additional information to clarify or supplement existing monitoring data.
- **Respond** to assessment findings by making decisions to either mitigate technical, management, and operational vulnerabilities; accept the risk; or transfer the risk to another authority.
- **Review and update** the monitoring program, revising the continuous monitoring strategy and maturing measurement capabilities to increase visibility into assets and awareness of vulnerabilities; further enhance data-driven control of the security of an organization's information infrastructure; and increase organizational flexibility.

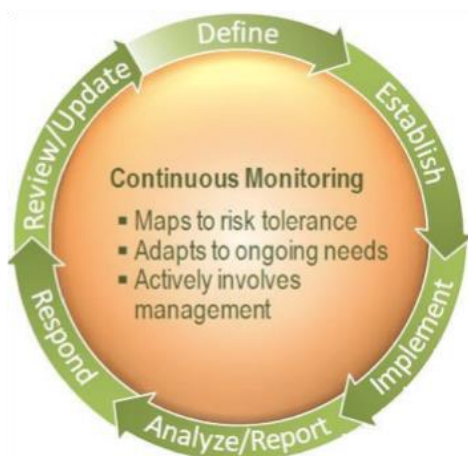


Figure 1. NIST SP 800-137 Continuous Monitoring Process

## 2. Continuous Monitoring Roles and Responsibilities

### 2.1 NEE Organizational Authorizing Official

The NEE designates an organizational Authorizing Official who is responsible for overseeing the security and privacy of the NEE IT system as well as the NEE's continuous monitoring activities. The AO must review all security artifacts provided by the NEE, the auditor, or CMS to ensure that the NEE's security and privacy risk posture remains effective for the organization's use of its IT system.

The AO ensures the organization is monitoring the Plan of Action & Milestones (POA&M) and reporting artifacts (such as vulnerability scan reports), as well as any significant changes associated with the NEE's service offering. The AO should use this information to make risk-based decisions about ongoing authorization of the system for that entity.

The NEE organization may be required to share pertinent security and privacy continuous monitoring artifacts with their upstream and downstream partners to help these entities make timely risk management decisions.

### 2.2 CMS Chief Information Security Officer

Although each NEE AO maintains the final approval authority for the use of a system by that entity, the CMS Chief Information Security Officer (CISO), or the delegated authority, acts as focal point for continuous monitoring activities of systems in operational status. The CMS CISO or the delegated authority is authorized to:

- Review continuous monitoring and security and privacy artifacts on a regular basis;
- Authorize, deny, monitor, suspend, and revoke a system's RTC as appropriate; and
- Authorize or deny significant change and deviation requests.

### 2.3 CCIIO Information System Security Officer

The CCIIO Information System Security Officer (ISSO) acts as the liaison for the CMS CISO to ensure that any NEEs in operational status strictly adhere to their established ISCM plan. The ISSO and the ISSO's support team are authorized to:

- Receive continuous monitoring and significant change artifacts on behalf of the CMS CISO;
- Perform initial analysis of artifacts, such as ensuring that scan reports and penetration tests correlate with POA&M submissions; and
- Facilitate CMS CISO review of artifacts.

## 2.4 Third-Party Independent Assessor Organization (Auditor)

Independent, third-party auditors must verify and validate the control implementation and test results for NEEs in the continuous monitoring process. Specifically, auditors are responsible for:

- Assessing the CMS-defined subset of the security and privacy controls annually;
- Submitting the assessment report to the NEE AO and CMS ISSO one year after the NEE's authorization date and each year thereafter;
- Performing announced penetration testing;
- Performing annual scans of web applications, operating systems/infrastructure, and databases; and
- Assessing changed controls on an ad hoc basis as requested by the NEE AOs or CMS for any changes made to the system.

To be effective in this role, auditors are responsible for ensuring that the chain of custody is maintained for any auditor-authored documentation. Auditors must also be able to vouch for the veracity and integrity of data provided by the NEE for inclusion in auditor-authored documentation. Documentation provided to the NEE must be placed in a format that either the NEE cannot alter or that allows the auditor to independently verify the integrity of the document. For example, if the NEE performs scans, the auditor either must be on site to observe the NEE performing the scans or be able to monitor or verify the results of the scans through other means documented and approved by the NEE AO.

## 3. Continuous Monitoring Process Areas

### 3.1 Operational Visibility

The NEE must demonstrate the efficacy of its continuous monitoring program through evidentiary information. After an authorization is approved, the NEE and its auditor must provide this evidence to the NEE AO in accordance with the stipulated timeframes. The timeframes may be at least monthly, annually, every three years, or as needed (please refer to Appendix B). The NEE AO relies on these evidentiary deliverables to evaluate the risk posture of the NEE's service offerings.

As part of the continuous monitoring process, CMS requires that an auditor perform an annual assessment of a subset of the overall security and privacy controls implemented on the NEE's IT system (please refer to Appendix C). The CMS ISSO may select additional controls for testing to assess the security and privacy risk posture based on the criteria in Table 1. The CMS ISSO has the option to vary the total number of controls tested to meet the desired level of effort for testing.

**Table 1. Control Selection Criteria**

| # | Criteria                                                      | Description                                                                                                                                                                                                                                         |
|---|---------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Conditions from previous assessment                           | Any conditions made by the CMS CISO, or authorized delegate, in the authorization letter or during a previous assessment. This includes the resolution of vulnerabilities within designated timeframes and implementation of new capabilities.      |
| 2 | Weakness identified since the last assessment                 | Any area where the system has known vulnerabilities or enhanced risk related to specific controls, such as an actual or suspected intrusion, compromise, malware event, loss of data, or denial of service (DoS) attack.                            |
| 3 | Known or suspected testing / continuous monitoring failure    | Any area where the IT system demonstrated a weakness or vulnerability in continuous monitoring or testing related to specific security controls, such as controls related to patch management, configuration management, or vulnerability scanning. |
| 4 | Control implementation that has changed since last assessment | Any control implementation that has changed since the last assessment must be independently assessed, even if it does not rise to the threshold of significant change.                                                                              |
| 5 | Newly discovered vulnerability, zero-day attack, or exploit   | Any control that is potentially affected by newly discovered vulnerabilities or zero-day exploits.                                                                                                                                                  |
| 6 | Recommendation of Authorizing Official or Organization        | Based on direct knowledge and use of an IT system, authorizing officials or organizations can require the NEE to test additional controls based on unique mission concerns or on the NEE's performance since their last assessment.                 |

Table 2 in Appendix B identifies the control frequencies for each continuous monitoring activity as well as the related deliverables. These deliverables include supplying evidence, such as providing monthly vulnerability scans of NEEs' operating systems / infrastructure, databases, and web applications.

## 3.2 Change Control

Because systems are dynamic, CMS anticipates that all systems are in a constant state of change. Configuration management and change control processes help maintain a secure baseline configuration of the NEE's architecture. Routine day-to-day changes are managed through the NEE's change management process described in its Configuration Management Plan.<sup>4</sup>

<sup>4</sup> NEEs participating in the Enhanced Direct Enrollment Program must follow the *Change Notification Procedures for Enhanced Direct Enrollment Entity Information Technology Systems* and the *Third-Party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements*.

At a minimum, the NEE change management process should include the following activities:

- Determining the nature of any significant changes<sup>5</sup> that includes, but is not limited to:
  - Supporting software changes or version upgrades
  - Adding services that modify the infrastructure
  - Modifying the connection to the CMS Data Services Hub
  - Responding to changes in the business process flow
  - Handling Personally Identifiable Information (PII) data creation, collection, disclosure, access, maintenance, storage, and use
  - Adding or modifying applications supporting ACA Exchange functions that may impact security and privacy
  - Adopting changes in Commercial Off-the-Shelf (COTS) software
  - Adapting to hardware or infrastructure changes, such as deployment of cloud technology
  - Changing operations at the processing site or outsourcing of data center operations
- Documenting the change following the NEE's organization change management process
- Assessing potential effects to information sharing
- Assessing potential effects to external system connections
- Completing a security impact analysis
- Reviewing the change and any impacts with all stakeholders
- Notifying CMS
- Testing all changes internally
- Coordinating required testing with CMS (changes with significant security and privacy impact will require auditor testing)
- Modifying all required documentation
- Updating legal agreements as required
- Approving the changes at the NEE AO level
- Coordinating production implementation

Many factors could make it difficult to establish specific thresholds for a significant change determination. For this reason, the NEE must involve the CMS ISSO and relevant business stakeholders in discussions related to any future changes to the system.

---

<sup>5</sup> Per NIST SP 800-37, significant changes to an information system may include, for example: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to system ports, protocols, or services; (iii) installation of a new or upgraded hardware platform; (iv) modifications to cryptographic modules or services; or (v) modifications to security controls. Examples of significant changes to the environment of operation may include, for example: (i) moving to a new facility; (ii) adding new core missions or business functions; (iii) acquiring specific and credible threat information that the organization is being targeted by a threat source; or (iv) establishing new/modified laws, directives, policies, or regulations.

The NEE must follow the *Change Reporting Procedures for NEE IT Systems*, including completing the *System Security and Privacy Change Notification (CN) Form*. Changes related to information sharing and external system connections will likely affect executed legal agreements, including the Business Agreement. Moreover, the ISA may require updates to the corresponding agreements, documentation, and artifacts. Proposed changes must be submitted to CMS ninety (90) days in advance of the planned implementation to allow time for change coordination, testing, and execution of new legal agreements, if necessary.

These IT system changes include any modifications to the IT systems to the extent that neither the CMS-approved audits nor the existing ISA are accurately reflected. Depending on the type, magnitude, or scale of the change, CMS may require resubmission of the RTC, which could take longer than sixty (60) days. The NEE AO, in coordination with the CMS ISSO, determines the assessment scope for the significant change within the NEE Security and Privacy Assessment Test Plan (SAP). The auditor should exercise best judgment to recommend the scope of the significant change assessment and coordinate the final scope with the NEE AO. Typically, if the significant change involves a new control implementation, the auditor must test the new control for the entire system. If the significant change is a new technology, the auditor must test its integration into existing controls.

If any anticipated change adds residual risk or creates other risk exposure that CMS finds unacceptable, CMS may revoke the system's authorization. For this reason, it is imperative that the NEE seek CMS approval before making the change. The goal is for the NEE to make planned changes in a controlled manner to avoid diminishing the security and privacy safeguards of the system.

After approval and implementation of the significant change, the NEE's auditor must perform an assessment and submit the NEE Security and Privacy Assessment Report (SAR) to CMS within the timeframe agreed by the NEE and CMS. The NEE must also submit updated documentation regarding the newly implemented changes.

### 3.3 Incident Response

NEEs must adequately respond to all security incidents and provide timely notification to all stakeholders. The CMS-NEE ISA requires NEEs to implement Breach and Incident Handling procedures that are consistent with CMS's Incident and Breach Notification Procedures and incorporate these procedures in the NEE's own written policies and procedures. As part of its Continuous Monitoring process, the NEE must routinely review and update its incident response and reporting procedures.

CMS may, at its discretion, direct the NEE to treat certain critical vulnerabilities as incidents, (e.g. zero-day vulnerabilities). NEEs must act immediately to fully resolve the vulnerability if possible or at least implement mitigating actions. The CMS ISSO may request immediate reporting on these critical vulnerabilities for NEE systems in operation. In addition, after an incident, the NEE must continue to track critical vulnerabilities in the system's POA&M even when the NEE is providing special reporting to CMS.

## 4. Continuous Monitoring Reporting Requirements

Once the NEE receives CMS RTC approval and authorization the NEE must submit the following compliance artifacts to CMS:

- **Quarterly** - POA&M submissions by the last business day of:
  - March
  - June
  - September
  - December

*Note: Unless there are outstanding weaknesses for which CMS would require monthly submissions until all major significant or major findings are resolved.*
- **Annual: (by the last business day of September)**
  - Annual Security and Privacy Assessment Report (SAR) of the CMS defined subset of security and privacy core controls;
  - Annual Penetration test results during reauthorization;
  - Annual System Security and Privacy Plan (SSP) updates;
  - Most recent three (3) months of the vulnerability scans; and
  - POA&M updates.

In addition to the CMS reporting requirements, the NEE must maintain the following internal activities:

- **Monthly:**
  - POA&M updates
  - Vulnerability scans
- **Quarterly:**
  - Continuous monitoring reports should follow the reporting requirements identified in SSP CA-7 Continuous Monitoring control
- **Annual:**
  - Annual System Security and Privacy Plan (SSP) updates

Refer to the Table 2, for a comprehensive list of internal NEE activities. An “X” in the “NEE-Authorized Deliverable” column indicates an internal NEE activity.

## Appendix A. Continuous Monitoring Reporting Summary

According to Security Control CA-7, Continuous Monitoring, the NEEs must provide reports of all vulnerability scans to their authorizing officials for review and must track these vulnerabilities within their POA&Ms. The analysis of these scan results should be performed in a manner consistent with a risk-based determination and authorization. Specifically, the NEE must:

- Document all inventory, late or deviated scan findings, and non-scan related findings in the POA&M (including low findings); all closed findings on the POA&M must be recorded for at least one year;
- Track each unique vulnerability as an individual POA&M item; and
- Submit and receive NEE AO approval for each deviation request or change to scan findings (e.g., risk adjustments, false positives, and operational requirements).

The NEE AO monitors these deliverables and other relevant artifacts monthly to ensure the NEE maintains an appropriate risk posture, which typically means the risk posture stays at the same level of authorization or better. As stated in its authorization letter, the NEE must maintain a continuous monitoring program.

Please refer to Appendix B, Table 2 for required deliverables to CMS. CMS's review and analysis of the NEE's continuous monitoring deliverables results in an annual continuous authorization decision by the CMS CISO or delegated authority.

## Appendix B. Control Action Frequencies

Security controls have different frequencies for performance and review, and some controls require review more often than others. Table 2 summarizes the minimally required frequencies needed for each continuous monitoring activity. Some activities require the NEE to submit a deliverable to CMS.

Other continuous monitoring activities do not require a deliverable and are reviewed by the auditor during security assessments. The NEE must demonstrate to the auditor that ongoing continuous monitoring capabilities are in place and are consistent with the NEE System Security and Privacy Plan (SSP). For example, if a NEE indicates in its SSP that it monitors unsuccessful login attempts on an ongoing basis, the auditor may ask to see log files, along with the NEE's analysis of the log files, for random dates over the course of a prior authorization period (e.g., bi-annual and annual).

For the security controls listed in Table 2, refer to the NEE SSP for a complete description of the control and the control implementation standards. An "X" in either the NEE-Authored Deliverable column or Auditor-Authored Deliverable column of Table 2 indicates that a deliverable is required.

The CMS ISSO may ask the NEE for a security artifact at any time, especially if the CMS ISSO has concerns about the security posture of the system. For example, if the NEE indicates in its SSP that it actively monitors information system connections, the CMS ISSO may ask the NEE to provide log file snippets for a specific connection at any point in time. If the CMS ISSO learns that an entity that connects to the NEE's system has been compromised by an unauthorized user, the CMS ISSO coordinates with the NEE to check in on the interconnection monitoring of the system. The NEE should anticipate that aside from scheduled continuous monitoring deliverables and CMS ISSO assessments, the CMS ISSO may request certain system artifacts on an ad hoc basis at any time.

The NEE is required to submit a schedule of activities to the CMS ISSO within forty-five (45) days from the date of its authorization and annually thereafter. This schedule assists NEEs in managing continuous monitoring activities.

**Note:** For controls that do not have an "X" in either the NEE-Authored Deliverable or Auditor-Authored Deliverable columns in Table 2, the NEE should be prepared to provide evidence of compliance upon request.

Table 2. Control Frequencies

| Control #              | Control Name                                                                   | NEE-Authorized Deliverable | Auditor-Authorized Deliverable | CMS Expected Deliverable | Comments |
|------------------------|--------------------------------------------------------------------------------|----------------------------|--------------------------------|--------------------------|----------|
| Continuous and Ongoing |                                                                                |                            |                                |                          |          |
| AC-2                   | Account Management                                                             |                            |                                |                          |          |
| AC-2(7)                | Account Management   Role-Based Schemes                                        |                            |                                |                          |          |
| CM-3                   | Configuration Change Control                                                   |                            |                                |                          |          |
| CM-6                   | Configuration Settings                                                         |                            |                                |                          |          |
| CM-8                   | Information System Component                                                   |                            |                                |                          |          |
| CM-8(1)                | Information System Component   Updates During Installations / Removals         |                            |                                |                          |          |
| CM-8(3)                | Information System Component   Automated Unauthorized Component Detection      |                            |                                |                          |          |
| IR-5                   | Incident Monitoring                                                            |                            |                                |                          |          |
| IR-6                   | Incident Reporting                                                             | X                          |                                |                          |          |
| SI-2                   | Flaw Remediation                                                               |                            |                                |                          |          |
| SI-2(3)                | Flaw Remediation   Time to Remediate Flaws / Benchmarks for Corrective Actions |                            |                                |                          |          |
| SI-3                   | Malicious Code Protection                                                      |                            |                                |                          |          |
| SI-4                   | Information System Monitoring                                                  |                            |                                |                          |          |
| AR-8                   | Accounting of Disclosures                                                      | X                          |                                |                          |          |

| Control #                                  | Control Name                                                                       | NEE-Authorized Deliverable | Auditor-Authorized Deliverable | CMS Expected Deliverable | Comments |
|--------------------------------------------|------------------------------------------------------------------------------------|----------------------------|--------------------------------|--------------------------|----------|
| <b>Every 24 hours</b>                      |                                                                                    |                            |                                |                          |          |
| AC-2(2)                                    | Account Management   Removal of Temporary / Emergency Accounts                     |                            |                                |                          |          |
| SI-7(1)                                    | Software, Firmware, and Information Integrity   Integrity Checks                   |                            |                                |                          |          |
| <b>Weekly</b>                              |                                                                                    |                            |                                |                          |          |
| AU-6                                       | Audit Review, Analysis, and Reporting                                              |                            |                                |                          |          |
| <b>Every 2 Weeks</b>                       |                                                                                    |                            |                                |                          |          |
| RA-5(5)                                    | Vulnerability Scanning   Privileged Access                                         |                            |                                |                          |          |
| <b>Every 30 Days / or within One Month</b> |                                                                                    |                            |                                |                          |          |
| CA-5                                       | Plan of Action and Milestones                                                      | X                          |                                | X <sup>6</sup>           |          |
| CA-7                                       | Continuous Monitoring                                                              | X                          |                                |                          |          |
| PE-8                                       | Visitor Access Records                                                             |                            |                                |                          |          |
| RA-5                                       | Vulnerability Scanning                                                             | X                          |                                | X <sup>7</sup>           |          |
| RA-5(2)                                    | Vulnerability Scanning   Update by Frequency / Prior to New Scan / When Identified |                            |                                |                          |          |
| SI-6                                       | Security Function Verification                                                     |                            |                                |                          |          |
| SI-7(1)                                    | Software, Firmware, and Information Integrity   Integrity Checks                   |                            |                                |                          |          |

<sup>6</sup> Monthly POA&Ms are due to CMS until the NEE resolves all significant or major findings. Thereafter, quarterly POA&M submissions are required as part of the ISCM activities. Closed findings must remain on the POA&M for at least one year.

<sup>7</sup> The most recent three months of vulnerability scans must be submitted to CMS during annual continuous authorization.

| Control #           | Control Name                                                    | NEE-Authorized Deliverable | Auditor-Authorized Deliverable | CMS Expected Deliverable | Comments |
|---------------------|-----------------------------------------------------------------|----------------------------|--------------------------------|--------------------------|----------|
| Every 60 Days       |                                                                 |                            |                                |                          |          |
| AC-2(2)             | Account Management   Removal of Temporary / Emergency Accounts  |                            |                                |                          |          |
| AC-2(3)             | Account Management   Disable Inactive Accounts                  |                            |                                |                          |          |
| IA-4                | Identifier Management                                           |                            |                                |                          |          |
| IA-5                | Authenticator Management                                        |                            |                                |                          |          |
| 90 Days / Quarterly |                                                                 |                            |                                |                          |          |
| AC-2                | Account Management                                              |                            |                                |                          |          |
| CA-7                | Continuous Monitoring                                           | X <sup>8</sup>             |                                | X <sup>9</sup>           |          |
| AC-22               | Publicly Accessible Content                                     |                            |                                |                          |          |
| CM-5(5)             | Access Restrictions for Change   Limit Production / Operational |                            |                                |                          |          |
| CM-7(1)             | Least Functionality   Periodic Review                           |                            |                                |                          |          |
| CM-7(4)             | Least Functionality   Unauthorized Software / Blacklisting      |                            |                                |                          |          |
| PE-3                | Physical Access Control                                         |                            |                                |                          |          |
| Every 6 Months      |                                                                 |                            |                                |                          |          |
| PE-2                | Physical Access Authorizations                                  |                            |                                |                          |          |
| PE-6                | Monitoring Physical Access                                      |                            |                                |                          |          |
| CP-9(1)             | Information System Backup   Testing for Reliability / Integrity |                            |                                |                          |          |

<sup>8</sup> Refer to SSP CA-7 Control Objectives and Implementation Standards.

<sup>9</sup> CMS expected deliverable includes the quarterly POA&M update and, as needed, the vulnerability scans.

| Control #         | Control Name                                   | NEE-Authorized Deliverable | Auditor-Authorized Deliverable | CMS Expected Deliverable | Comments |
|-------------------|------------------------------------------------|----------------------------|--------------------------------|--------------------------|----------|
| 365 Days Annually |                                                |                            |                                |                          |          |
| AC-2              | Account Management                             |                            |                                |                          |          |
| AC-17             | Remote Access                                  |                            |                                |                          |          |
| AT-2              | Security Awareness Training                    |                            |                                |                          |          |
| AT-3              | Role-Based Security Training                   |                            |                                |                          |          |
| AU-1              | Audit and Accountability Policy and Procedures | X                          |                                |                          |          |
| AU-2(3)           | Audit Events   Reviews and Updates             |                            |                                |                          |          |
| CA-2              | Security Assessments                           |                            | X                              | X                        |          |
| CA-6              | Security Authorization                         | X                          |                                | X <sup>10</sup>          |          |
| CA-7              | Continuous Monitoring                          |                            |                                |                          |          |
| CA-7(1)           | Continuous Monitoring   Independent Assessment |                            |                                |                          |          |
| CA-8              | Penetration Testing                            |                            | X                              | X                        |          |
| CM-2(1)           | Baseline Configuration   Reviews and Updates   |                            |                                |                          |          |
| CM-8              | Information System Component                   |                            |                                |                          |          |
| CM-9              | Configuration Management Plan                  | X                          |                                |                          |          |
| CP-2              | Contingency Plan                               | X                          |                                |                          |          |
| CP-3              | Contingency Training                           |                            |                                |                          |          |

<sup>10</sup> NEE submission to CMS includes:

- Annual Security and Privacy Assessment Report (SAR) of the CMS-defined subset of security and privacy core controls (Appendix C)
- Annual Penetration Test results for continuous authorization
- Annual System Security and Privacy Plan (SSP) updates
- Most recent three months of the vulnerability scans
- POA&M updates

| Control # | Control Name                                               | NEE-Authorized Deliverable | Auditor-Authorized Deliverable | CMS Expected Deliverable | Comments |
|-----------|------------------------------------------------------------|----------------------------|--------------------------------|--------------------------|----------|
| CP-4      | Contingency Plan Testing                                   | X                          |                                |                          |          |
| IR-2      | Incident Response Training                                 |                            |                                |                          |          |
| IR-3      | Incident Response Testing                                  |                            |                                |                          |          |
| IR-8      | Incident Response Plan                                     | X                          |                                |                          |          |
| PL-2      | System Security Plan                                       | X                          |                                | X                        |          |
| PL-4      | Rules of Behavior                                          |                            |                                |                          |          |
| PS-2      | Position Risk Designation                                  |                            |                                |                          |          |
| PS-6      | Access Agreements                                          |                            |                                |                          |          |
| RA-3      | Risk Assessment                                            |                            |                                |                          |          |
| RA-5      | Vulnerability Scanning                                     |                            | X                              | X                        |          |
| SC-7(4)   | Boundary Protection   External Telecommunications Services |                            |                                |                          |          |
| AR-4      | Privacy Monitoring and Auditing                            |                            |                                |                          |          |
| AR-5      | Privacy Awareness and Training                             |                            |                                |                          |          |
| DI-1      | Data Quality                                               | X                          |                                |                          |          |
| DM-1      | Minimization of Personally Identifiable Information        | X                          |                                |                          |          |
| SE-1      | Inventory of Personally Identifiable Information           | X                          |                                |                          |          |
| SE-2      | Privacy Incident Response                                  | X                          |                                |                          |          |
| TR-1      | Privacy Notice                                             | X                          |                                |                          |          |
| UL-2      | Information Sharing with Third Parties                     | X                          |                                |                          |          |

| Control #     | Control Name                                                | NEE-Authorized Deliverable | Auditor-Authorized Deliverable | CMS Expected Deliverable | Comments |
|---------------|-------------------------------------------------------------|----------------------------|--------------------------------|--------------------------|----------|
| Every 2 Years |                                                             |                            |                                |                          |          |
| AR-1          | Governance and Privacy Program                              | X                          |                                |                          |          |
| 3 Years       |                                                             |                            |                                |                          |          |
| AC-1          | Access Control Policy and Procedures                        | X                          |                                |                          |          |
| AT-1          | Security Awareness and Training Policy and Procedures       | X                          |                                |                          |          |
| AU-1          | Audit and Accountability Policy and Procedures              | X                          |                                |                          |          |
| CA-1          | Security Assessment and Authorization Policy and Procedures | X                          |                                |                          |          |
| CM-1          | Configuration Management Policy and Procedures              | X                          |                                |                          |          |
| CM-3          | Configuration Change Control                                |                            |                                |                          |          |
| CP-1          | Contingency Planning Policy and Procedures                  | X                          |                                |                          |          |
| IA-1          | Identification and Authentication Policy and Procedures     | X                          |                                |                          |          |
| IA-4          | Identifier Management                                       |                            |                                |                          |          |
| IA-5          | Authenticator Management                                    |                            |                                |                          |          |
| IR-1          | Incident Response Policy and Procedures                     | X                          |                                |                          |          |
| MA-1          | System Maintenance Policy and Procedures                    | X                          |                                |                          |          |
| MP-1          | Media Protection Policy and Procedures                      | X                          |                                |                          |          |

| Control # | Control Name                                                | NEE-Authorized Deliverable | Auditor-Authorized Deliverable | CMS Expected Deliverable | Comments |
|-----------|-------------------------------------------------------------|----------------------------|--------------------------------|--------------------------|----------|
| PE-1      | Physical and Environmental Protection Policy and Procedures | X                          |                                |                          |          |
| PL-1      | Security Planning Policy and Procedures                     | X                          |                                |                          |          |
| PL-2      | System Security Plan                                        | X                          |                                |                          |          |
| PS-1      | Personnel Security Policy and Procedures                    | X                          |                                |                          |          |
| RA-1      | Risk Assessment Policy and Procedure                        | X                          |                                |                          |          |
| RA-3      | Risk Assessment                                             |                            |                                |                          |          |
| SA-1      | System and Services Acquisition Policy and Procedures       | X                          |                                |                          |          |
| SA-15     | Development Process, Standards, and Tools                   |                            |                                |                          |          |
| SC-1      | System and Communications Protection Policy and Procedures  | X                          |                                |                          |          |
| SI-1      | System and Information Integrity Policy and Procedures      | X                          |                                |                          |          |
| AR-2      | Privacy Impact and Risk Assessment                          |                            |                                |                          |          |

## Appendix C. Annual Assessment of Security and Privacy Controls

As part of the continuous monitoring process, the NEE is required to have an auditor perform an annual assessment of a subset of the overall security and privacy controls implemented on the IT system as documented in Table 3. The CMS ISSO may select additional controls for testing to assess the security and privacy risk posture based on evolving threats and demonstrated weaknesses. The CMS ISSO has the option to vary the total number of controls tested to meet the desired level of effort for testing.

**Table 3. Security and Privacy Controls to Be Tested Annually**

| Control #                                         | Security / Privacy Control Name                          |
|---------------------------------------------------|----------------------------------------------------------|
| <b>Access Control (AC)</b>                        |                                                          |
| AC-1                                              | Access Control Policy and Procedures                     |
| AC-2                                              | Account Management                                       |
| AC-3                                              | Access Enforcement                                       |
| AC-5                                              | Separation of Duties                                     |
| AC-6                                              | Least Privilege                                          |
| AC-10                                             | Concurrent Session Control                               |
| AC-11                                             | Session Lock                                             |
| AC-12                                             | Session Termination                                      |
| AC-17                                             | Remote Access                                            |
| <b>Audit and Accountability (AU)</b>              |                                                          |
| AU-2                                              | Audit Events                                             |
| AU-6                                              | Audit Review, Analysis, and Reporting                    |
| <b>Security Assessment and Authorization (CA)</b> |                                                          |
| CA-3                                              | System Interconnections                                  |
| CA-5                                              | Plan of Action and Milestones                            |
| <b>Configuration Management (CM)</b>              |                                                          |
| CM-2                                              | Baseline Configuration                                   |
| CM-3                                              | Configuration Change Control                             |
| CM-4                                              | Security Impact Analysis                                 |
| CM-6                                              | Configuration Settings                                   |
| CM-7                                              | Least Functionality                                      |
| CM-7(2)                                           | Prevent Program Execution                                |
| CM-7(4)                                           | Unauthorized Software/Blacklisting                       |
| <b>Identification and Authentication (IA)</b>     |                                                          |
| IA-2                                              | Identification and Authentication (Organizational Users) |
| IA-2(1)                                           | Network Access to Privileged Accounts                    |
| IA-2(2)                                           | Network Access to Non-Privileged Accounts                |

| Control #                                        | Security / Privacy Control Name                              |
|--------------------------------------------------|--------------------------------------------------------------|
| IA-5                                             | Authenticator Management                                     |
| IA-5(1)                                          | Password-Based Authentication                                |
| IA-8                                             | Identification and Authentication (Non-Organizational Users) |
| IA-8(2)                                          | Acceptance of Third-Party Credentials                        |
| <b>Incident Response (IR)</b>                    |                                                              |
| IR-5                                             | Incident Monitoring                                          |
| IR-6                                             | Incident Reporting                                           |
| IR-8                                             | Incident Response Plan                                       |
| IR-9                                             | Information Spillage Response                                |
| <b>Media Protection (MP)</b>                     |                                                              |
| MP-4                                             | Media Storage                                                |
| MP-5(4)                                          | Cryptographic Protection                                     |
| MP-6                                             | Media Sanitization and Disposal                              |
| <b>Planning (PL)</b>                             |                                                              |
| PL-2                                             | System Security Plan                                         |
| PL-4                                             | Rules of Behavior                                            |
| <b>Risk Assessment (RA)</b>                      |                                                              |
| RA-5                                             | Vulnerability Scanning                                       |
| <b>System and Services Acquisition (SA)</b>      |                                                              |
| SA-4                                             | Acquisition Process                                          |
| SA-9                                             | External Information System Services                         |
| <b>System and Communications Protection (SC)</b> |                                                              |
| SC-7                                             | Boundary Protection                                          |
| SC-8                                             | Transmission Confidentiality and Integrity                   |
| SC-13                                            | Cryptographic Protection                                     |
| SC-23                                            | Session Authenticity                                         |
| SC-28                                            | Protection of Information at Rest                            |
| <b>System and Information Integrity (SI)</b>     |                                                              |
| SI-2                                             | Flaw Remediation                                             |
| SI-3                                             | Malicious Code Protection                                    |
| SI-4                                             | Information System Monitoring                                |
| SI-4(1)                                          | System-Wide Intrusion Detection System                       |

| Control #                                              | Security / Privacy Control Name                  |
|--------------------------------------------------------|--------------------------------------------------|
| <b>Accountability, Audit, and Risk Management (AR)</b> |                                                  |
| AR-2                                                   | Privacy Impact and Risk Assessment               |
| AR-8                                                   | Accounting of Disclosures                        |
| <b>Security (SE)</b>                                   |                                                  |
| SE-1                                                   | Inventory of Personally Identifiable Information |
| <b>Use Limitation (UL)</b>                             |                                                  |
| UL-2                                                   | Information Sharing with Third Parties           |