

Continuous Diagnostics and Mitigation

CDM and the Risk Management Framework

Learning Community Event

February 18, 2016



Homeland
Security

Federal Network Resilience

Table of Contents

- I. Introduction 3**
- II. Meeting Summary 4**
 - A. Synergies between Continuous Diagnostics and Mitigation and Risk Management Framework 4
 - B. Transitioning to Automated Assessments 4
 - C. Workforce Engagement and Communication Prior to Implementation 5
 - D. Inventorying Assets 5
 - E. Challenges for Asset Management 6
 - F. Ongoing Authorization 6
 - G. Enforcing Systems Behind on Fixing Critical Issues 7
 - H. Addressing Legacy Systems 7
 - I. Additional Resources 7
- III. Appendices 8**
 - A. Meeting Agenda 8

I. Introduction

The National Institute of Standards and Technology's (NIST) [Risk Management Framework](#) (RMF) provides organizations with a holistic, risk-based approach to categorizing information and information systems, selecting and implementing appropriate security controls for an information system, assessing the effectiveness of the security controls (initially and via continuous monitoring), and authorizing the information system to operate. The Continuous Diagnostics and Mitigation (CDM) Program, which defines security capabilities and provides tools to identify cybersecurity vulnerabilities on an ongoing basis, supports the automated assessment and monitoring of implemented security controls. The six RMF steps are:

1. Categorize information system.
2. Select security controls.
3. Implement security controls.
4. Assess security controls.
5. Authorize information system.
6. Monitor security controls.

The U.S. Department of Homeland Security (DHS) Federal Network Resilience (FNR) Division Learning Program hosted a virtual Learning Community Event (LCE) on February 18, 2016, to help agencies understand the relationship between the RMF and CDM Program implementation. The FNR Learning Program invited three subject matter experts to participate in a panel discussion and facilitate breakout sessions on specific RMF topics.

The panelists included:

- **Kelley Dempsey**, Information Systems Security Specialist, NIST
- **Ann Marie Keim**, Assessment and Accreditation Official, National Aeronautics and Space Administration (NASA) Kennedy Space Center
- **Kimberly Hennings**, Director of Cyber Security; Compliance, Audits, Policy & Enforcement; U.S. Department of Agriculture (USDA)

The topics covered in the panel discussion and breakout session included:

- Understanding CDM through the RMF.
- Using [NIST Special Publication \(SP\) 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems](#) to enable more seamless CDM Program implementation.
- Using the [NIST Internal Report \(IR\) 8011: Automation Support for Security Control Assessments](#) to support the transition to automated assessments and monitoring.
- Communicating throughout the organization to prepare for CDM Program implementation.
- Addressing challenges with asset inventory and management.
- Designing strategies for ongoing authorization.
- Remediating systems that are behind on fixing critical issues.
- Implementing the RMF and CDM Program in legacy systems.

II. Meeting Summary

A. Synergies between Continuous Diagnostics and Mitigation and Risk Management Framework

The CDM Program is a dynamic approach to fortify the cybersecurity of government networks and systems. It provides Federal agencies with the capabilities and tools to conduct automated, ongoing assessments. The CDM Program enables Federal agencies to expand their continuous diagnostic capabilities by increasing the capacity of their network sensors, automating the collection of data from sensors, and prioritizing risk alerts.

The CDM Program will aid in RMF step 2, task 2 and 3, where organizations must develop their continuous monitoring strategy. The CDM Program will also help automate the security control assessment processes that support the ongoing authorization concept, under which assessment and authorization (A&A) activities, formerly conducted every three years, transition into A&A activities conducted with the frequencies specified in the organizations' continuous monitoring strategy. Implementing the CDM Program as part of the RMF helps organizations collect information on security control status and make ongoing determinations of whether or not the risk of operating an information system is acceptable.

Prioritizing aspects of the RMF has helped some agencies implement the CDM Program. For instance, at NASA, the ongoing A&A through the continuous monitoring module is currently a priority and is now on a test server being tested internally. Following that test, NASA will also explore other capabilities to enhance the CDM Program and RMF, including IBM BigFix agents that leverage most of their devices. The USDA is considering test pilots for some of their agencies as well, and hopes to gain information and lessons learned throughout the process that can inform other implementations.

Cloud computing is also being discussed with regard to CDM. Currently, the CDM Program does not address cloud security improvements; however, work is currently in progress for a CDM Program security solution in this area.

B. Transitioning to Automated Assessments

Kimberly Hennings engineered the transition model at USDA from a traditional, primarily manual A&A process to ongoing assessments. She designed the model to be iterative/cyclical so that there was no expectation on staff to complete it at once. To ensure the entire enterprise was represented in implementation, USDA engaged multiple working groups and integrated project teams that included client technology services and multiple agencies and offices. She shared key aspects of the transition:

- One of the challenges was associating costs to assessments, which USDA accomplished by measuring the level of effort per assessment activity.
- As a transitional step, USDA segmented the assessment process into thirds. Each third (i.e., assessment period) focused on a specific set of key controls.
 - The working groups were responsible for aligning the controls to each assessment period.
 - The working groups had representatives from 29 USDA agencies and offices and were responsible for developing determination statements and what key controls should be assessed each period.

The [NISTIR 8011](#): *Automation Support for Security Control Assessments* can support automated assessments, and ties defect checks to security control from [NIST SP 800-53](#): *Security and Privacy Controls for Federal Information Systems and Organizations*:

- There will be NISTIR 8011 volumes for each of the CDM Security Capabilities. The first two have been completed and released for public draft:
 - NISTIR 8011 Volume 1 provides an overview of the automation of security control assessments, including CDM, and provides an explanation of how to use the remaining volumes.
 - NISTIR 8011 Volume 2 identifies the security controls are associated with managing Hardware Assets and maps those controls to defect checks and attack steps.
- NIST SP 800-53 Revision (Rev) 5 is now open for pre-draft comments until April 1.
 - The initial public draft will be distributed via the Federal Information Security Management Act (FISMA) list and GovDelivery distribution lists and posted to the [NIST Website](#) in early fall 2016.

C. Workforce Engagement and Communication Prior to Implementation

Participants recognized that culture and organizational politics can affect the level of staff participation in new processes. Working groups led by information technology (IT) professionals can help organizations educate their workforce on RMF and CDM. Working groups allow for openness within agencies, enabling organizations to transparently discuss implementation issues and other problems.

Communication throughout organizations will aid in gathering information from several agencies, which can be used to share solutions and best practices and to discuss problems affecting the implementation of RMF and/or the CDM Program. Participants shared examples of successful engagement:

- Susan Hansche of FNR noted that at the Department of State (DOS), during her experience observing the implementation of iPOST (an automated assessment program with a centralized dashboard), it took time for the employees to realize the potential of the program. The organization was successful by implementing a risk scoring system that promoted decision-making; encouraged involvement from the Information System Security Officers (ISSOs) and system administrators; and used internal listservs to help distribute information.
- Another participant noted that iPOST did not resonate with staff at first because people felt they could not adjust the scores. When users understood they could use exceptions and risk transfers, they then felt the scoring system was fair, and this helped to create the “buy-in” the organization needed.
- Another participant noted that employees are paying attention because they know there is a payoff and it works. The organization has a goal-oriented process that is communicated, and it seeks commitment memos from its departments that indicate if they are out of compliance and what their milestone dates are.
- A participant mentioned that there was no rollout as of yet in the classified environment.

D. Inventorying Assets

The Office of Management and Budget (OMB) requires all information systems to be inventoried. Organizations that are unable to provide full system inventories due to financial and time constraints would need to work these problems out with the Inspector General (IG) and OMB, based on established directives.

CDM Program tools will assist in scanning organizational networks for assets (i.e., components or devices) that can help the organization ensure that all information system components are known and thus be appropriately managed. In addition, all physical assets should be associated with a single information system.

E. Challenges for Asset Management

Participants shared challenges their agencies are experiencing and lessons learned during one of the breakout sessions:

- NASA currently uses Dell KACE, yet many of the **devices do not have an automation capability or are isolated**, so they have to be manually updated. The information is only as good as organizational inputs.
 - NASA can compare its inputs with Foundstone and Nessus scans to see what has not been reported along with the Domain Name System (DNS).
 - Asset management and the waiver process are a heavy lift for some organizations, so the authorizing official may have to accept some risk (on a temporary basis).
 - Some problems arise specifically with how certain devices (e.g., firewalls, routers) will be inventoried.
 - NASA formerly used PatchLink, and Dell KACE will have to be replaced with IBM BigFix; however, the organization does not yet know how to transition without impacting business.
 - NASA is hoping to leverage Group B lessons learned for future implementations.
- **Dealing with dynamic subsystems remains a challenge.** It is difficult to know when to phase out the systems as they reach end of their lifecycle.
- The Federal Election Commission has experienced **issues collecting assets and controlling procurement**. The organization started using Nessus and Tenable Security Center to collect compliance and vulnerability data and to identify passive vulnerabilities to identify and establish a link between assets.
- One participant noted that his agency's big challenge is that **many contractors have systems connected to theirs, but no place for centralized control** or cybersecurity awareness for all of them. Organizations are responsible for managing system interconnections and for ensuring contractors receive required training. These are all security controls found in the low impact baseline.
- Another participant from the U.S. Department of the Interior (DOI) noted that the **CDM Program enabled them to see multiple tools, but did not work for asset management**. IBM BigFix, however, is now helping to make asset management easier.

F. Ongoing Authorization

The discussion focused on how often to assess controls for Ongoing Authorization (OA) and how agencies are thinking about this process. OA requires automated continuous monitoring, which cannot happen without a robust strategy. There is no longer the three-year static process for A&A. Depending on the environment, organizations will assess some controls more frequently and other controls less frequently. As a result, assessment periodicity is now dependent on organization timeframes. When fully operational, the CDM Program defect checks will provide visibility into the majority of the information system security controls to provide a more timely understanding of the status of each information system security control. It all depends on the control volatility, Plan of Action and Milestones (POA&Ms) on that

control, and other variables that may cause an agency to want to check more frequently to provide the most current information. [NIST SP 800-137: Information Security Continuous Monitoring for Federal Information Systems and Organizations](#) provides more information on determining appropriate security control assessment frequencies.

The frequency for ongoing authorization itself (using input from automated security control assessments) is based on time-driven triggers, but may also be based on event-driven triggers. See the [Supplemental Guidance on Ongoing Authorization](#) for more information on time- and event-driven triggers.

G. Enforcing Systems Behind on Fixing Critical Issues

The discussion noted that monthly score cards can be used to indicate information systems that are behind on fixing critical issues. Further, it is important to develop department-level buy-in with metrics for OA, so that any shortfalls can be tied to annual performance evaluations. The CDM Dashboard is currently under development to provide visibility to critical issues associated with agency systems. This will enhance an agency's ability to evaluate what issues are affecting systems and how to prioritize fixing them.

H. Addressing Legacy Systems

The panelists discussed issues associated with irreplaceable legacy systems and noted that “air gaps” will continue to exist. Individual agencies are evaluating how to address legacy systems that cannot fully support areas automated assessments and monitoring. As the CDM Program progresses, communication across agencies will become important for solving these problems.

I. Additional Resources

These resources will help agencies implement automated security control assessments:

- **CDM Bits and Bytes Email Newsletter.** Provides weekly CDM tips, information for upcoming CDM events, and updates on new CDM resources. Register here: <https://www.us-cert.gov/cdm/home>.
- **Federal Risk Scoring Sub-Working Group.** Develops risk scoring for the CDM Program, and is looking for input from cybersecurity professionals. Contact cdm.fnr@hq.dhs.gov for more information.
- **National Cybersecurity Workforce Framework.** Provides educators, students, employers, employees, training providers, and policy makers with a systematic and consistent way to organize, think, and talk about cybersecurity work, including what is required of the cybersecurity workforce: <https://nices.us-cert.gov/training/national-cybersecurity-workforce-framework>.
- **NIST Computer Security Resource Center.** Provides information on NIST publications: <http://csrc.nist.gov/>. Click here to view the initial public draft of NISTIR 8011: <http://csrc.nist.gov/publications/PubsDrafts.html>.
- **US-CERT Portal.** Helps government users share threat information: <https://portal.us-cert.gov/>.
- **US-CERT Website.** Provides additional CDM information, including CDM resources, event information, and meeting summaries: <https://www.us-cert.gov/>.

Submit any questions, ideas for future meetings, or comments to cdm.fnr@hq.dhs.gov.

III. Appendices

A. Meeting Agenda

TIME	ACTIVITY
10:45-11:00	Panelists Arrive
11:00-11:15	Participants Arrive; Networking and Getting to Know Your Avatar
11:15-11:20	Agenda Review and Introduction <ul style="list-style-type: none">• Overview of the session and rules of engagement
11:20-11:40	Panelist Self-Introductions <i>Kelley Dempsey, NIST</i> <i>Ann Marie Keim, NASA's Kennedy Space Center</i> <i>Kimberly Hennings, USDA</i>
11:40-12:05	Question and Answer with Panelists <ul style="list-style-type: none">• Pre-defined questions from the moderator• Audience members ask questions from virtual podium
12:05-12:25	Breakout Sessions – Each breakout session is led by a panelist and focuses on providing a discussion around a specific topic that caters to the panelist's expertise.
12:25-12:40	Breakout Session Presentations – Each panelist presents the main takeaway from each of the breakout sessions.
12:40-12:50	Closing Statements from the Panelists – Moderator summarizes the meeting and asks each panelist to provide their closing thoughts.
12:50-1:00	Wrap-up and Thank You <i>Patrick White, Nexight Group LLC</i>