FORCE3
A SIRIUS COMPANY

DEMYSTIFYING THE CDM PROGRAM

TO STRENGTHEN CYBERSECURITY ACROSS THE FEDERAL GOVERNMENT

In 2013, the Department of Homeland Security (DHS) introduced the Continuous Diagnostic and Mitigation (CDM) Program in an effort to help the 23 CFO Act civilian agencies and non-CFO Act agencies fortify their security posture and fill any gaps. The program is designed to help these agencies identify cybersecurity risks on an ongoing basis, prioritize those risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.

As the program approaches its seventh year, agencies across the federal government are beginning to fully understand and utilize the program as the DHS continues to enhance and improve it. However, confusion and uncertainty still exist among federal CIOs, and there are underlying concerns that need to be overcome for agencies to realize the benefits of the ambitious program.

WHAT IS THE CDM PROGRAM?

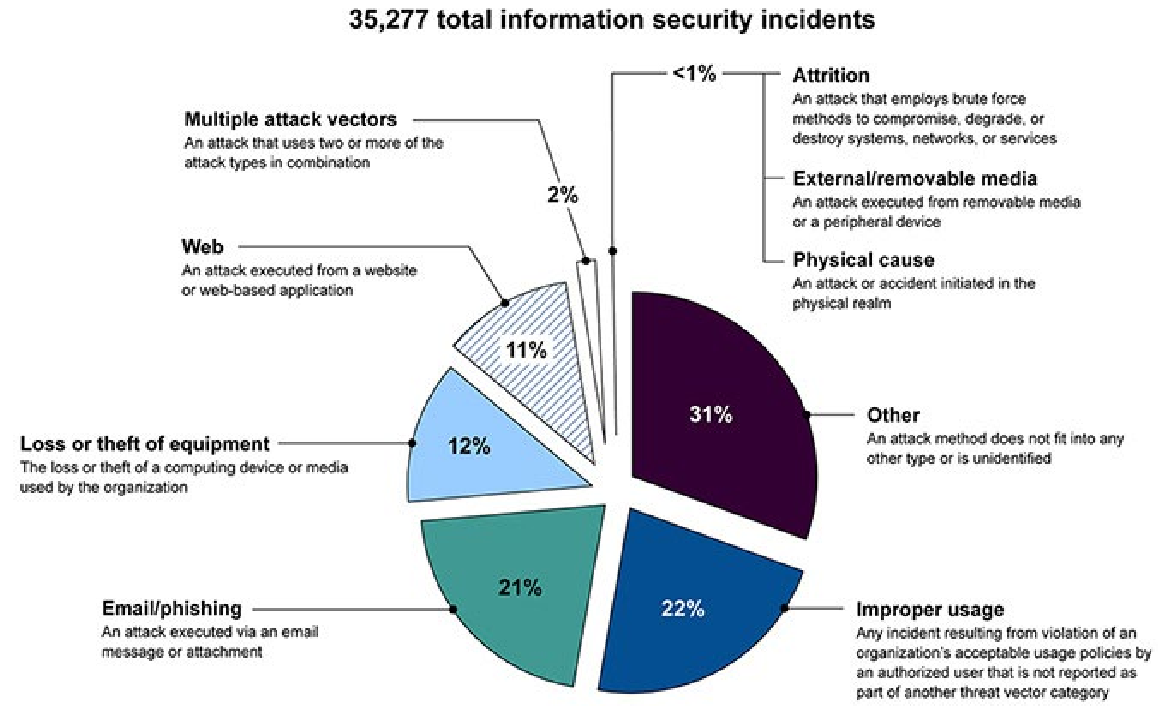
The origins of the CDM program start with the mission of the Department of Homeland Security:

> “With honor and integrity, we will safeguard the American people, our homeland, and our values.”

Safeguarding the American people and our homeland includes safeguarding information. The federal government has a vast amount of information on our most critical infrastructure and the American public, which is under constant threat from both outside and inside forces. In 2017, more than 35,000 security incidents[1] were reported to the DHS by federal agencies.

Technology teams across the federal government face constraints in adopting and implementing new security technology to protect against threats. If they do have the latest technology, it may not be implemented across their entire enterprise. They also may not have the resources to continuously monitor their systems and fully utilize their tools to detect and stop cyberattacks or spot trends.

To further complicate the security landscape, each agency has their own technology teams, and within each agency, different departments may have conflicting needs and priorities. For the DHS, whose mission is to protect the American people and our homeland as a whole, getting a holistic picture of security across civilian agencies is challenging – each agency has their own network using a variety of tools with a varying level of knowledge and budget. With no comprehensive view, finding ways to support agencies and help them defend against the ongoing threats to our government systems is increasingly difficult.



Source: GAO analysis of United States Computer Emergency Readiness Team and Office of Management and Budget data for fiscal year 2017. | GAO-18-622

This is where the CDM program comes in. It was designed to remove the barriers faced by federal technology teams across civilian agencies, to offer teams the additional support of the DHS, and to provide DHS with a more comprehensive view of threats against federal technology systems.

RESEARCHED AND APPROVED TECHNOLOGY – AND THEY COVER THE COSTS

With technology changing rapidly and resources – both human and budgetary – being stretched thin, DHS set out to vet technology tools and determine which ones would support the government's cybersecurity needs. They developed a list of approved technology to guide agencies towards proven tools that would help them strengthen their security posture.

DHS then sweetened the deal – if an agency needs a tool to support their cybersecurity efforts that is on their approved list, they can get the cost of that technology covered by the CDM program. This saves the agency time in dealing with procurement contracts and allows them to allocate their budget to other pressing needs. Agencies also don't have to hold off on purchasing needed security technology until a new budget cycle. For DHS, with more agencies using the CDM program to acquire their technology, they can get better cost structures and realize savings with bulk purchases.

ADOPTION AND IMPLEMENTATION – A PHASED APPROACH

Purchasing technology is one thing. Implementing, optimizing, monitoring, and maintaining it is something else.

Finding – and stopping – cyber threats and attacks against the government is a monumental task, and one that can overwhelm an individual agency's IT teams, whose responsibilities go beyond cybersecurity to keep their agency operating smoothly on a daily basis.

The CDM program supports agencies with a roadmap to implement and optimize the right security tools for that agency, automate processes, and monitor activity in real time.

THE PHASES OF CDM

DHS has introduced the CDM program in phases – which are the same phases agencies need to follow to strengthen their security measures and realize the full benefits of the CDM program support and real-time dashboards.

PHASE 1

ASSET MANAGEMENT

PHASE 2

IDENTITY AND ACCESS MANAGEMENT

PHASE 3

NETWORK SECURITY MANAGEMENT

PHASE 4

DATA PROTECTION MANAGEMENT

With each phase, technology teams strengthen their security across their enterprise in a logical progression. DHS has completed the introduction of phases 1 – 3, and are in the process of introducing phase 4. Several civilian agencies can be found in various stages of each phase, with some nearing completion of phase 3, while others only in the early stages of phase 1 or not even on the implementation path.

1 ASSET MANAGEMENT: WHAT IS ON THE NETWORK?

In order to protect a network, CIOs need to understand exactly what is on it.

During Phase 1, sensors discover everything connected to the network. Agencies can then focus on problem areas and gaps, and deploy security tools that automate hardware and software asset management, configuration settings, and common vulnerability management capabilities.

The Office of Personnel Management (OPM) was the first agency to fully implement Phase 1 of CDM after a data breach in 2015.

2 IDENTITY AND ACCESS MANAGEMENT: WHO IS ON THE NETWORK?

Once CIOs know what is on their network, they need to know who is accessing it. In Phase 2, sensors look for access points and privilege protocols. Agencies can then configure security tools to handle privilege management and monitor users on their networks. These tools can also detect whether users are engaging in unauthorized activity, and spot unusual trends in behaviors.

> “The use of CDM has set the stage for OPM to move into a continuous monitoring approach that enhances OPM’s ability to manage its systems and continually to evolve its systems security in real time,”

said **David Garcia**, OPM’s CIO at a hearing on CDM with the House Homeland Security Committee.

> “OPM has made use of CDM technologies to identify and strategically resolve potential vulnerabilities, which has resulted in better overall risk management and response.”

3 NETWORK SECURITY MANAGEMENT: WHAT IS HAPPENING ON THE NETWORK?

Moving into Phase 3, agencies can assess their network security and activity, find security gaps both at the perimeter and inside, and deploy automated tools to monitor their network and identify any threats of anomalies.

4 DATA PROTECTION MANAGEMENT: HOW IS DATA PROTECTED?

Phase 4 provides insights and tools to protect data at rest, in transit, and in use to prevent data loss and manage events.

As agencies progress through implementing each phase, technology teams gain access to more information that is fed into easy-to-read dashboards updated in real time. DHS achieves their goal of fortifying the cybersecurity of civilian government networks and systems as a whole, reducing threat surfaces, increasing visibility into the federal cybersecurity posture, and improving federal response capabilities.

THE CDM PROGRAM DASHBOARDS

During each phase, agencies install and deploy sensors across their systems. These sensors perform automated scans and searches. They look for gaps in security, which agencies can then fill with approved technology acquired through the CDM program.

With the sensors and the new technology installed, data is fed into easy-to-use dashboards that give agency technology teams visibility into what is happening across their network. The dashboards receive, aggregate, and display information, which alerts IT teams to issues, risks, and attacks.

This data also feeds into a federal level dashboard, which offers enterprise-wide insights into cybersecurity risks and responses occurring across all participating federal agencies, thus giving DHS an overall status check.

With the easy to use dashboards that collect information on an ongoing basis through an automated process, IT teams are empowered to respond to any discovered gaps, threats, and attacks.

An added benefit of the dashboards is they help agencies meet Federal Information Security Modernization Act (FISMA) reporting.

WHY AGENCIES SHOULD PARTICIPATE IN THE CDM PROGRAM

DHS notes that “the CDM Program enhances government network security through automated control testing and progress tracking.” The program provides support services to implement sensors and dashboards. Agencies get near-real time results for better security, and it helps them identify and mitigate flaws. The CDM program also lowers operational risk. Additionally the CDM program fulfills Federal Information Security Management Act (FISMA) mandates. The program was designed to support agencies in the most effective and efficient way without taking control over an agency’s security, leaving that to individual agency technology teams to still maintain and manage.
The question is really why aren’t agencies adopting the CDM program, and how do they overcome the barriers?

BARRIERS TO ADOPTION

The CDM Program offers federal agencies security tools and real-time dashboards the agencies determine they need at no cost to them. Why hasn't every agency implemented the program?

DATA CONTROL

When an agency implements security tools received through the CDM program, their data gets added to a combined federal dashboard created by DHS. The individual agency dashboards are also generated out of DHS. CIOs who are already looking at improving their network security are hesitant to "give up" control of their data to an "outside" entity.

While they are sharing their data with the DHS, they are gaining access to tools that support them to control their own data. DHS is serving as an extension of the agency's technology teams – they are another set of eyes to stop threats. They can see across the government landscape for a holistic view, and recommend learnings from one agency to another. The program also ensures data privacy. Data sent to DHS by CDM participants does not include information about specific department or agency computers, applications, or user accounts. All civilian federal agencies are on the same team, and working together makes the entire federal systems stronger – and more secure.

EXISTING TECHNOLOGY

Many agencies have already implemented security tools they feel are working across parts of their network they don't want to replace with the technology offered by the CDM program.

The CDM program does not require dismantling existing functionality. The sensors spot gaps in the agency, and offer recommendations for filling those gaps. Existing technology that is already modernized can be kept in place, and new technology can be added through the program that can be integrated with current technology.

THE PHASED APPROACH

The CDM program follows a phased approach, starting with Phase 1, and going step-by-step through to the Phase 4. There is no going backwards or skipping a phase.

While some agencies may see this as a loss of control over their security roadmap, the phases follow a logical approach. Information discovered and resolved in each phase supports the activities in the next phase.

> "Going out of order would create gaps instead of resolving them."

TOO MANY VENDORS

When the sensors detect issues, agencies can look at the approved product list and choose the tools that would work best for them. The approved list is long though, and the number of vendors is growing. The agency still needs to determine which product would work best for their specific issue and their agency while also integrating with existing functionality.

This is where a solution provider can support agencies. Good solution providers work closely with the latest technology and are strong partners with the manufacturers. They can look at the agency's existing functionality, review the data from the sensors, and recommend the technology solution that would work best to resolve the issue or fill the gap. Solution providers can also support implementation of the tool and integration with the existing framework.

The barriers to adoption are not insurmountable. Threats against federal agencies will continue to rise and become more sophisticated. The CDM program is an excellent way for agencies to get the tools, support, and information they need to secure their network.

CDM PROGRAM WINS: A LESSON FROM THE SBA

The Small Business Administration (SBA) recently completed a successful pilot[3] of the CDM program that focused on connected devices to their network, which they included as part of their cloud migration strategy. With so many employees in the field supporting small businesses around the country, they were an early adopter of moving data to the cloud to ensure field staff had easy, secure access to the data they needed. But with that access came a need to secure their endpoints, and to have full visibility about who and what is connected to their network at any time of day. They turned to the CDM program. Working through the phases, they implemented new technology to address concerns, and developed a custom dashboard for around-the-clock monitoring of every device connected to their network. They now have a real-time view who is accessing their network for what information. They can stop any unknown entity before it becomes a problem.

The CDM program adoption was part of SBA's overall IT transformation strategy, which they started in 2018. Because security touches everything related to technology across an agency, participating in the CDM program was a way for SBA to access additional resources and to build and test security functionality with the other technology improvements that were being put in place with their cloud migration activity.

Through all of their efforts. The SBA was one of the few agencies to receive an A on the June 2019 Fitara Scorecard for Modernizing Government Technology. The CDM program worked well for them.

GETTING STARTED

The government continues to invest in the CDM program to enhance, improve, and expand it. Just recently, the CDM Program was expanded[4] to include state and local governments to help them secure their systems against the ransomware attacks that are occurring across the country. The program is breaking down traditional barriers and silos that exist between federal agencies and local entities – who are all on the same team with the same goals – to keep this country and the American people safe from threats.

Regardless if you are ready to jump on board or hesitant to use the program, talking to a service provider about your current security landscape if a good first step. The service provider can help with the implementation of the sensors, recommend the right tools based on the sensor findings, implement those tools, then integrate and optimize them across your network. They can also offer ongoing support in reading dashboard findings and responding to threats. Service providers act as an extension of your technology team.

Force 3 a technology solutions provider that has worked with the federal government providing IT solutions and services for over 25 years. As the network security company, Force 3 understands the security requirements needed in the federal space and partners with leading manufacturers. Security is woven into everything we do. Whether you are just thinking about participating in the CDM program, are ready to join, or are already working through the phases, Force 3 can help.

FORCE 3
A SIRIUS COMPANY

Contact us today for a **free one-hour consultation** about the current state of your network security.

Force 3
2151 Priest Bridge Drive
Crofton, MD 21114
1 (800) 391-0204

[1] *"Cybersecurity Challenges Facing the Nation – High Risk Issues" US Government Accountability Office, https://www.gao.gov/key_issues/ensuring_security_federal_information_systems/issue_summary*

[2] *Miller, Jason. "Rep. Hurd says CDM is Software Implementation Problem, He's Only Partly Correct." Federal News Network April 2, 2018*

[3] *Heckman, Jory. "SBA Wraps up CDM Pilot as Part of Enterprise IT Transformation." Federal News Network September 23, 2019*

[4] *Corrigan, Jack. "As State and Local Governments Face Rising Cyber Threats, The Legislation Would Give them Free Access to Tools Provided Under the Continuous Diagnostics and Mitigation Program." NextGov October 23, 2019*