CONTINUOUS DIAGNOSTICS AND MITIGATION IN THE DYNAMIC AND EVOLVING FEDERAL ENTERPRISE

EXECUTIVE SUMMARY

As securing federal networks becomes increasingly critical due to mounting threats and new risks brought on by digital transformation, federal agencies have a responsibility to bolster their defenses by taking advantage of the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) Program. By helping agencies use new and existing technologies to enable continuous network monitoring and automate detection and remediation, a well-designed CDM solution will have a very real impact on cybersecurity.

Instead of viewing CDM as an unnecessary compliance chore, agencies should embrace it as a cost-effective means for securing and evolving their digital transformations. As CDM moves into Phase 3, which focuses on what is happening on agency networks, agencies are advised to work with proven cybersecurity vendors that are offering best-of-breed solutions.

STRENGTHENING CYBERSECURITY IN FEDERAL GOVERNMENT

Hardening federal agency networks is a national priority of utmost importance. On March 15, 2018, DHS and the Federal Bureau of Investigation (FBI) issued a joint alert on Russian government actions targeting U.S. government entities.[1] Although the multistage intrusion campaign did not specifically compromise government networks, it gained remote access to critical control systems at power plants after targeting small commercial facilities' networks with malware and spear phishing.

Of course, this is just one of many examples where nation-states or individual actors have successfully hacked systems. In this new digital era, protecting the information systems of federal networks and infrastructure—from business systems to operational technology such as dams and electrical grids—is job one for federal agency CISOs. Given the opportunity, would-be attackers from terrorist groups, foreign governments, or even our own citizenry could identify and exploit vulnerabilities to cause major damage. Federal agencies must do a better job of managing and securing their systems, including oversight and reporting, to mitigate risk.

While human security expertise is always needed, the speed at which cyber threats are delivered presents the real and persistent challenge of detecting and mitigating threats in real time. To address constantly evolving cyber threats in real time, automation and continuous network monitoring are essential. Agencies must enable systems and networks to share intelligence, act, and respond without manual intervention. While it is impossible for CDM to close all gaps, it does enable centralized reporting of network activity—with automated responses when applicable—thus freeing security professionals' time to respond to infrastructure vulnerabilities.

70% of federal networks **have now been breached.**[2]

57% have been **breached in the past year.**[2]

Network Visibility and Control: How CDM Can Help

The federal government's CDM Program is a dynamic approach to fortifying the cybersecurity of government networks and systems. The federally funded program was established by Congress to provide federal agencies with capabilities and tools to identify cybersecurity risks on an ongoing basis, prioritize risks based on potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. Agency CDM dashboards connect to federal dashboards to enable automated risk reporting, which is essential to strengthening military .mil and civilian .gov networks against attack.

The government has divided CDM into four phases, with the first two phases concentrating on asset and event management to answer the question, "What and who is on the network?" To give agencies more flexibility to fill gaps for the first two phases and move on to Phase 3, DHS and the General Services Administration (GSA) created a new task order called DEFEND (Dynamic and Evolving Federal Enterprise Network Defense) under the Alliant Governmentwide Acquisition Contract (GWAC). This gives agencies a standardized vehicle for cost-effective purchase and deployment of additional resources, as well as easy access to vendors that understand CDM.[3]

As many agencies move into Phase 3—namely, the question, "What is happening on the network?"—they will focus on boundary protection and incident response. Phase 3 involves more extensive and dynamic monitoring of security controls, requiring agencies to improve integration between network security and infrastructure components to prevent the lateral spread of threats.[4] Phase 4 will concentrate on data protection to support overall CDM program goals.

With many agencies moving into Phase 3, now is the perfect time for them to enhance network security through automated control testing and progress tracking. According to DHS, when done properly, a CDM approach can:

- Provide services to implement sensors and dashboards
- Deliver near-real-time results
- Prioritize the worst problems within minutes, versus quarterly or annually
- Enable defenders to identify and mitigate flaws at network speed
- Lower operational risk and exploitation of government IT systems and networks
- Fulfill Federal Information Security Management Act (FISMA) mandates for federal cyber investments[5]

An Opportunity for Digital Transformation

Most agencies grappling with CDM are in the midst of a digital transformation and infrastructure modernization: the adoption of mobility, Internet of Things (IoT), and cloud solutions to connect data and stakeholders, drive innovation, and improve efficiency. However, digital transformation brings its own operational challenges: lack of visibility and control, borderless networks, more sophisticated threats, security gaps, and a larger attack surface.

Interfacing with other government networks and systems—a primary goal of CDM—also introduces risk. Using disparate point products to solve these problems makes automation difficult. Without automation, significant resources and time are needed, making CDM expensive and complex to manage.

Agencies should couple their digital transformation initiatives with CDM to create a holistic, integrated security framework that provides network-wide visibility and threat intelligence sharing. Taking a piecemeal approach can widen potential attack windows and prolong remediation efforts. Cloud and mobile strategies must be evaluated simultaneously to understand what additional steps need to be taken to provide comprehensive network and data security.

As DHS and other federal agencies adopt cloud services, CDM updates will naturally follow. Guidance should be provided on how to understand where data is/how it's protected and how to identify potential security gaps that can lead to vulnerabilities. Ultimately, though, the strength and effectiveness of an agency's cybersecurity posture is the agency's responsibility. Cyber threat actors will be sure to capitalize on the gaps that such updates to the CDM program may seek to address.

> "We found a **75% increase** in terms of the total number of assets [agencies have on their networks] once we got automated tools into the environment."[6]
>
> – Kevin Cox,
> CDM Program Manager, Department of Homeland Security

Compliance Considerations

Although CDM is more about combatting real-time threats as opposed to historical compliance reporting, demonstrating compliance is still essential. Agencies should keep in mind, however, that there's a difference between compliance and security: one can be compliant and still have security gaps.

Much of the pain agencies experience around compliance begins with their ability to easily demonstrate compliance. Demonstrating compliance can be challenging because it requires aggregating logs and reports from multiple systems. This process is often a manual one and can take significant amounts of time to properly assess, architect, and implement—time that agencies rarely have. Where possible, agencies should invest their time wisely to thoroughly assess their present ability to demonstrate compliance and address any discovered deficiencies.

72-Hour Window

To assess the state of a network and mitigate all threats.

The CDM initiative currently calls for a 72-hour window to completely assess the state of an agency's network on a recurring basis—putting the "continuous" in CDM—and this is no small task. Just a few of the considerations regarding CDM's 72-hour assessment window include:

- Security patching must be addressed on a 72-hour mitigation window, regardless of the size of the agency's network.
- Proper system prioritization must be performed within the 72-hour window to allow for timely mitigation of discovered threats. In other words, the more critical a system, the faster its needs must be identified and addressed.
- Risk evaluations must be conducted to properly identify the controls necessary to mitigate any discovered threats in a demonstrably timely fashion that adheres to CDM's stated goal of completely assessing a network within a 72-hour window, which must consider the following six steps:
    1. Install/update sensors
    2. Automated search for flaws
    3. Collect results from departments/agencies
    4. Triage and results analysis
    5. Fix worst findings first
    6. Report progress of assessment/remediation

Federal agency leaders are responsible for managing heterogeneous enterprise-class networks that must be secured with federal government-approved controls and are constantly available. More often than not, an agency's technical staff members are typically "burning the candle at both ends" just to keep up with their pre-CDM mandated tasks. They also face the challenge of architecting a solution that provides persistent transparency of traffic processed across the entire agency's network and adheres to CDM's 72-hour assessment/mitigation window. Considering that devices across federal agency networks are often of a heterogeneous nature and are rarely, if ever, designed to natively communicate with each other, the challenge to meet CDM's mandate becomes resoundingly clear.

Federal agencies need solutions that are fully automated and purpose-designed to collect, process, and disseminate intelligent alerts and reports from dissimilar systems. CDM's challenges are best met with solutions that are developed with native integration as a carefully designed standard, not as an afterthought.

A well-designed, CDM-compliant solution needs to integrate security elements from different systems in a fashion that effectively automates compliance tracking and reporting across each of them—in as close to real time as possible. While CDM's mandate for continuous 72-hour network assessments is a necessary and welcome step forward, a truly effective CDM-compliant solution needs to be better from the start. Implementing a solution that simply meets this mandate without the ability to exceed it has the very real potential of falling behind the malware threat curve quickly and negates an agency's considerable investment in time, budget, and human capital to achieve CDM compliance. An effective CDM solution should enable an agency's ability to proactively detect concerted cyberattacks against their organization, not only for today's threats, but for tomorrow's as well.

As an important stepping stone, federal agencies should seek CDM solutions that provide real value in assessing their needs to comply with various federal government regulations and/or certifications all at once. Some of these critical regulations include:

CDM Approved Products List. All products deployed as part of CDM must be approved by DHS and listed on the CDM Approved Products List (APL). In August 2017, the CDM program grandfathered in approximately 70,000 products covering software, hardware, and services, allowing agencies to combine existing investments with new solutions to mature their continuous monitoring programs.

NIST. 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. Beginning in Phase 3, CDM must fit into the NIST RMF, which recommends six steps that are critical for implementing an effective cybersecurity program for federal agencies:

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

When evaluating solutions to enhance security controls, agencies should ask vendors about their NIST mappings and capabilities to meet NIST guidance. Specifically, NIST 800-53 Rev. 4 addresses the ability to take inventory of authorized and unauthorized devices on the network.

NIST also provides guidance on enabling a more seamless CDM program implementation through NIST Special Publication (SP) 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems. For help with the transition to automated assessments and monitoring, agencies should refer to NIST Internal Report (IR) 8011: Automation Support for Security Control Assessments.

FISMA. CDM helps federal agencies automate the FISMA reporting process with agency-level CDM dashboards that securely route information to the federal dashboard. These, in turn, are reported to the CyberScope data reporting application managed by DHS.[7] Eventually, the goal is to move the federal government from yearly FISMA compliance to continuous security improvement, thereby eliminating expensive recertification requirements.[8]

CDM has the potential to make FISMA more relevant with automated, near-real-time scanning and validation of network and system security. Since much of the information collected and fed to agency CDM dashboards will meet FISMA requirements, agencies can cut down on manual, paper-based reporting processes.[9]

Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure/ Modernizing Government Technology Act. The executive order issued by President Donald Trump in 2017 underscores the importance of cybersecurity to the federal government, making it clear that "agency heads will be held accountable by the president."[10] In some commercial cases, such as the high-profile Equifax breach, top executives have stepped down and faced potential fines.

> "It's not that hard to protect the core of the network—the challenge is in making sure the seams are sewn shut. It's the interfaces between the disparate systems that pose great risk."[11]
>
> – Stan Tyliszczak,
> Chief Engineer, General Dynamics IT

Conclusion

According to a recent survey of 100 IT security professionals from U.S. federal agencies, 68% believe they are "very" or "extremely" vulnerable to a data breach, up from 48% the year before.[12] CDM represents a new approach to cybersecurity that can help federal agencies address these vulnerabilities by gaining real-time visibility. Ultimately, CDM will help agencies analyze critical security-related information faster while continually monitoring networks, which allows security staff to address vulnerabilities as the threat landscape evolves.

A Pressing Need

44% more

unmanaged, non-cataloged devices were found on civilian federal networks than expected during Phase 1 CDM.[13]

Given the very real threats to government networks—and potentially impactful consequences—agencies have a responsibility to stay current with CDM phases to make sure they get the most value from the program. Thanks to CDM DEFEND, agencies have a significant amount of flexibility and autonomy in deciding on their preferred CDM solutions while still being able to leverage DHS funding.

[1] "Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," U.S. Computer Emergency Readiness Team, March 15, 2018.
[2] "2018 Thales Data Threat Report Federal Government Edition," Thales e-Security, February 22, 2018.
[3] Jason Miller, "Two acquisition events mark the turning point for the CDM program," Federal News Radio, August 28, 2017.
[4] "Department of Homeland Security Selects Booz Allen Hamilton as Prime Contractor on $621M Task Order to Enhance Cybersecurity Across Federal Government," Booz Allen Hamilton, February 2, 2018.
[5] "Continuous Diagnostics and Mitigation (CDM)," Department of Homeland Security, accessed March 16, 2018.
[6] "CDM Finding Application on Both Sides of the Adoption Spectrum," MeriTalk, March 23, 2018.
[7] "CDM Frequently Asked Questions," General Services Administration, accessed March 16, 2018.
[8] Faisal Shirazee, MSNS, CISSP, "FISMA reporting and NIST guidelines," accessed March 16, 2018.
[9] "With CDM, What Happens to FISMA?" accessed April 3, 2018.
[10] Donald J. Trump, "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 11, 2017.
[11] Tobias Naegele, "CDM Program Starts to Tackle Complexities of Cloud," GovTechWorks, January 31, 2018.
[12] "Thales: U.S. Federal Government Agencies experience more than 20% increase in data breaches," PR Newswire, February 22, 2018.
[13] Shaun Waterman, "DHS cyber tool finds huge amount of 'shadow IT' in U.S. agencies," CyberScoop, April 13, 2017.