Mighty Guides

CDM FROM THE FRONTLINES

CISOs, PMs and Others Share Success Perspectives and Lessons Learned

tenable™

TABLE OF CONTENTS

Mighty Guides

Mighty Guides make you stronger.

These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you. Reading a Mighty Guide is kind of like having your own team of experts. Each heartfelt and sincere piece of advice in this guide sits right next to the contributor's name, biography, and links so that you can learn more about their work. This background information gives you the proper context for each expert's independent perspective.

Credible advice from top experts helps you make strong decisions. Strong decisions make you mighty.

FOREWORD

As federal cybersecurity programs have matured, federal agencies have moved from periodic assessments of static security controls to continuous monitoring of IT resources and activities. The U.S. Department of Homeland Security (DHS) supports this evolution through its Continuous Diagnostics and Mitigation (CDM) program, which provides federal departments and agencies with risk-based, cost-effective capabilities that identify ongoing cybersecurity risks, prioritize those risks based on potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.

This e-book contains insight from conversations with government program participants and cybersecurity industry leaders who have first-hand experience dealing with CDM program requirements. They provide an array of perspectives. We asked these professionals about the challenges they have encountered in implementing and operating under the CDM program and how they overcame them. The result of those discussions is the excellent advice you'll find here regarding the activities that led to their successes with the program.

We hope you'll find these insights and best practices from the frontlines valuable and that you can use them to achieve success as you implement and support CDM in your own organization.

Regards,
Amit Yoran
CEO, Tenable

tenable™

Tenable™, Inc. is the Cyber Exposure company. Over 23,000 organizations of all sizes around the globe rely on Tenable to manage and measure their modern attack surface to accurately understand and reduce cyber risk. As the creator of Nessus®, Tenable built its platform from the ground up to deeply understand assets, networks and vulnerabilities, extending this knowledge and expertise into Tenable.io™ to deliver the world's first platform to provide live visibility into any asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, large government agencies and mid-sized organizations across the private and public sectors. Learn more at tenable.com.

INTRODUCTION

The CDM program, established by the U.S. Department of Homeland Security in 2013, is designed to help governmental agencies take an enterprise approach to cybersecurity. In other words, it is designed to help them map hardware and software assets, harden configurations and settings, and continuously monitor boundaries. For some government agencies, the move to CDM hasn't been easy.

In an effort to pull together strategies and best practices for successful CDM rollouts, we reached out to 10 cybersecurity experts who have either actively been involved with the CDM program or have consulted with agencies as they moved through the phases of CDM. We asked these professionals the following questions:

Federal agencies have been working hard to comply with each phase of DHS's CDM program. Have you encountered challenges? If so, how have you overcome them? What best practices or advice would you like to share that led to your greatest successes with the program?

The insight in the pages that follow covers everything from planning a rollout to creating a strong foundation and changing cultural beliefs. These experts agree that CDM is a valuable program, and we hope you'll find the wisdom collected here helps you move smoothly and successfully through its phases.

All the best,
David Rogelberg
Publisher

One big challenge for many organizations now implementing CDM is how to change their security culture from a focus on compliance to a focus on risk management.

LinkedIn

JEREMIAH CLIFTON

Information Security Architect, Major U.S. city

THE RIGHT RESOURCES ENSURE CDM SUCCESS

RENEE FORNEY
CEO,
Forney Group

Renee Forney is the CEO of the Forney Group and the executive managing director of Global Cyber Security Management at Equinoxys. She is a cybersecurity thought leader with an emphasis on cyber workforce, cyber intelligence and enterprise risk management. Renee previously served as deputy chief information officer for Cybersecurity and Enterprise Operations at the U.S. Department of Energy. Prior to DOE, she was the U.S. Department of Homeland Security's executive director for the Cyber Skills Management Support Initiative.

Twitter | Website | LinkedIn

"The U.S. Department of Homeland Security has done a great job establishing the CDM framework and its associated tools," says Renee Forney, chief executive officer of the Forney Group. Forney, who is the former deputy chief information officer of Cybersecurity and Enterprise Operations at the U.S. Department of Energy (DOE), was also at DHS during the development of CDM, so she has a unique perspective on the program and what it's designed to accomplish.

"The ultimate responsibility for implementation lies with the agencies," she says, pointing out that that's often where the problems crop up. "The agencies are complex, and often, the responsibilities at the end point levels are distributed across an agency's enterprise. One difficulty is the lack of awareness at the practitioner level." Forney says that information often doesn't trickle down from the management level, which creates that lack of awareness.

KEY LESSONS

1. **Create a solid communication plan, and make sure that everyone, from management to practitioner, is in on the conversation so that they'll understand what's being asked of them.**

2. **Create a team whose only job is to attend to the activities and requirements of CDM to increase your chances for success.**

> *"You're building a plane and trying to fly it at the same time. You're resource constrained, as well, so you have the same people doing both those things."*

THE RIGHT RESOURCES ENSURE CDM SUCCESS

One way Forney educated all the DOE personnel involved was to create a working group that included both leaders and practitioners. “Educate that group about what CDM is all about—the benefits and barriers to reaching those benefits,” she suggests. “Putting together the working group really helps you move through the CDM phases. Keep in mind that you’re building a plane and trying to fly it at the same time. You’re resource constrained, as well, so you have the same people doing both those things.”

“A working group also helps because a lot of process reengineering and change management go along with the implementation of CDM,” Forney points out. “You have a workforce that’s coming out of the three-ring binder environment. Now, they have to do things differently. The working group helped us establish communication channels.” Those channels, she explains, were important to helping people understand that the new way of doing things was not only easier, but more efficient.

According to Forney, “It’s also important that the contracting staff coming in has a good understanding and knows not only the as-is state of the environment, but also the to-be environment because often we have to contract for resources to support this migration into CDM. Making sure that you have a dedicated implementation team is key. It’s difficult to implement CDM and perform other duties as assigned.”

“What human resources?” Forney asks as an example. “You must know not just the technical tools you’re buying. but the people you’ll need to implement the program fully. Make sure that you’re looking far enough down the road that you can build future needs into your budget requests.”

Forney’s final explanation of the importance of working groups and future planning put things into perspective: “You have to make implementation a priority. For CDM rollout to be successful, it must be resourced properly.”

> *“You have to make implementation a priority. For CDM rollout to be successful, it must be resourced properly.”*

The strength of the CDM program is that the control categories are prioritized according to the Critical Security Controls. Phase 1 consists of the basic asset inventory/configuration management/vulnerability assessment capabilities that provide the minimum required foundation for any successful cybersecurity program. However, they also require cooperation and often change with the IT operations group. All CDM success stories involve a CISO/program lead who is able to work with the CIO or IT operations management ahead of procuring CDM tools.

Twitter | Website

JOHN PESCATORE

Director, SANS Institute

LONG-TERM GOALS GUIDE CDM SUCCESS

MARK WEATHERFORD

SVP and Chief Cybersecurity Strategist,
vArmour

Mark Weatherford is SVP and Chief Cybersecurity Strategist at vArmour. He has more than 20 years of security operations leadership and executive-level policy experience in some of the largest and most critical public and private sector organizations in the world, including roles at The Chertoff Group, Deputy Under Secretary for Cybersecurity at DHS, VP & CSO at the North American Electric Reliability Corporation (NERC), and CISO for the states of California and Colorado.

Twitter | Website | Blog | LinkedIn

Prior to becoming senior vice president and chief cybersecurity strategist at vArmour, Mark Weatherford ran the cybersecurity program at the U.S. Department of Homeland Security. There, he hired John Streufert from the U.S. Department of State to come to DHS and design what became the CDM program. "The idea was that we would create a program that each federal agency could—but didn't have to—participate in. We wanted to give agencies visibility into their networks," Weatherford explains. "As we developed the program, we realized that there were significantly more security features we could build into the overall CDM solution."

Federal agencies today still have the choice not to participate in the program. In some instances, it might even be better for them to use the CDM strategies to purchase technologies outside the program. "The problem is, technology changes faster than the government is able to absorb change. Even today, as agencies look at Phases 2 and 3 of CDM, technology has evolved past what they're trying to do with CDM right now."

KEY LESSONS

1. **A long-term technology strategy starts with clear vision into existing capabilities. When you have that clear view, you can map the most logical path to the future.**

2. **Network visibility highlights technological weaknesses. Once you know those weaknesses, then you can select the best solution to address them.**

"The biggest problem was trying to build a technology stack that wasn't one-size-fits-all because every agency has its own requirements, mission and standards."

LONG-TERM GOALS GUIDE CDM SUCCESS

Weatherford says if he were in a government agency today, he would respond to the quandary of outdated technology by "understanding the technical components of the overall CDM program, and then looking at what's available today. The technologies for sale on the CDM contract may not always be the latest versions. You might be able to find something better without going through the CDM program." After all, understanding your technology is the purpose of CDM Phase 1.

"From the beginning," Weatherford says, 'The biggest problem was trying to build a technology stack that wasn't one-size-fits-all because every agency has its own requirements, mission and standards. Every federal agency is different. That's why the program went with multiple vendors, multiple contractors and multiple security products."

The idea was to get ahead of technology so that agencies weren't installing outdated applications and programs. "This is part of the federal acquisition problem. The government is always behind in technology procurement because of the technology acquisition process." To overcome this problem, Weatherford suggests remembering that "each prime contractor selected a variety of technologies to solve the CDM issue." From his perspective, Weatherford says it's possible that "agencies may not need to look at the entire CDM solution, but rather, single technology components that meet their specific needs." It's what he would do if he were in their shoes and had the option to buy the most up-to-date version of a technology without going through the standard government procurement process.

The main thing to remember is the goal of the program. "The goal was always to create a long-term strategy for the federal government." That starts with creating visibility into existing networks because, as Weatherford points out, "It isn't until you know where you are that you can build a solid framework for where you want to be."

> *"It isn't until you know where you are that you can build a solid framework for where you want to be."*

Despite the emphasis on automation in the CDM program, manpower remains a critical challenge in effective continuous monitoring. No one tool does everything and agency IT staff already stretched thin will have to implement, manage and respond to a suite of tools that generate large volumes of data and numerous alerts.

Twitter | Website

WILLIAM JACKSON

Writer, The Tech Writers Bureau

TRAINING: THE OVERLOOKED IMPERATIVE FOR SUCCESSFUL CDM

KEVIN SANCHEZ-CHERRY

Cybersecurity Policy, Architecture and Training Lead,
U.S. Department of Transportation

Kevin Sanchez-Cherry (CISSP) is the Cybersecurity Policy, Architecture and Training lead for the U.S. Department of Transportation's (DOT) Office of Cybersecurity and Information Assurance. He is a senior advisor to the DOT CISO on cybersecurity policy, training and workforce management. Prior to DOT, Kevin served in a variety of cybersecurity positions for such agencies as the U.S. Department of Education, the U.S. Secret Service, and the Financial Industry Regulatory Authority.

LinkedIn

"Looking at it from the policy side," says Kevin Sanchez-Cherry, "I need to ensure that the policies related to CDM are in line with the capabilities of the systems we have in place—that they're achievable, feasible and measurable. It doesn't do any good to have a policy for CDM if we don't have any way to enforce or monitor it."

To help ensure that policies and capabilities are synced, Sanchez-Cherry says that he stays in contact with the operations teams and those responsible for testing and installing new applications. He makes sure that everyone knows his or her responsibilities within the new systems.

The U.S. Department of Transportation is currently in Phase 2 of CDM, and Sanchez-Cherry says that looking back, "I would suggest that there needs to be more than buy-in from senior management. Senior management must really understand what the program is, what its capabilities are and what it's supposed to do. There must be full communication to avoid misconceptions."

KEY LESSONS

1. **Management and key stakeholders need to understand the extent and implications of any new integrations or installations so that they can champion their success.**

2. **Training is an essential element of installation or upgrade success—one that should be practiced repeatedly and often.**

> *"I need to ensure that the policies related to CDM are in line with the capabilities of the systems we have in place—that they're achievable, feasible and measurable."*

"There should also be full communication at each step with stakeholders beyond those who are going to set up and configure the apps and those who will be monitoring day-to-day interactions so that they understand what's going on and what their responsibilities are."

Sanchez-Cherry's message is to prepare people. "As agencies move forward, they should not only consider the result of implementation, but also look at supporting policies and any training that stakeholders and support staff involved in the project, however peripherally, will need."

Sanchez-Cherry cites an agency he used to work with as an example. "They significantly overhauled part of the infrastructure—did a lot of much-needed rework on hardware and software. But, there was no funding for training." The result, Sanchez-Cherry says, may be chaos. "In a few years, they may be in the same situation as before the infrastructure was redesigned."

"You must have training for the people who will maintain, operate and monitor your upgrades." Sanchez-Cherry goes on: "Training is not just a one-time event. It has to be ongoing. Software and hardware are upgraded, and the staff members who work with those systems need an 'upgrade,' too."

Overall, Sanchez-Cherry says, "We've gotten past the rough phase, where the team was reviewing our infrastructure and comparing it with the desired state. Now, we're humming along nicely."

"Software and hardware are upgraded, and the staff members who work with those systems need an 'upgrade,' too."

CDM was my vision when I served as deputy undersecretary for Cybersecurity at DHS. I had seen iPost, which John Streufert developed when he was CISO at the U.S. Department of State, and wanted to do the same thing on a federal scale. I immediately hired John at DHS after I was appointed. Humorous anecdote: CDM was originally called the Continuous Monitoring Program, but some people were concerned about using the term monitoring—as in monitoring people—so we changed it to CDM.

Twitter | Website | Blog | LinkedIn

MARK WEATHERFORD

SVP & Chief Cybersecurity Strategist, vArmour

SCALE MAKES A DIFFERENCE IN CDM IMPLEMENTATIONS

BRIAN ZEITZ

Medical Center CIO,
U.S. Department of Veterans Affairs

Brian Zeitz is the Medical Center CIO for the U.S. Department of Veterans Affairs in Cincinnati, Ohio. As CIO, Zeitz leads IT specialists who maintain voice, video and data for the Medical Center and six clinics. He and his team ensure that 5,319 users dispersed throughout 23 buildings possess the IT tools necessary to care for America's veterans. Previously, Zeitz was the program manager for International Cyber Operations at the U.S. Department of Homeland Security.

LinkedIn

The CDM implementation story varies considerably from one federal agency to another. Based on head count, the U.S. Department of Veterans Affairs (VA) Veterans Health Administration (VHA) is by far the largest federal agency implementing CDM. VHA's network is broken down into 22 Veterans Integrated Services Networks (VISNs). Brian Zeitz, a facilities chief information officer for VA based in Cincinnati, Ohio, works within VISN 10. "There are 360,000 people in VA," Zeitz explains. "More than 95 percent of these are in VHA, which delivers health services to veterans. VISN 10 supports five medical centers in Ohio and six in Michigan. My organization supports the Cincinnati area, which hosts a 10-story hospital, 6 clinics, a community living center, and 3,000 VA employees."

KEY LESSONS

1. **VA's biggest challenge has been the sheer size of the agency.**
2. **VA's Phase 1 implementation will be complete when administrators can look at something on the network and quickly see whether it's normal or not.**

"I believe we're at CDM Phase 1. We're finding out interesting things we never knew about how data flow on our network. What we're doing now is defining normal."

SCALE MAKES A DIFFERENCE IN CDM IMPLEMENTATIONS

Many factors can affect how an agency approaches its CDM implementation. For instance, the National Oceanic Atmospheric Administration (NOAA) is a smaller agency with a global network and a lot of publicly shared data. In contrast, the Federal Bureau of Investigation (FBI) handles a great deal of highly classified data that cannot be shared even with other government agencies. Strict rules govern who can access the data, and legal requirements determine the life cycle of some types of data. Zeitz says, "NOAA and FBI have very different data and access management challenges, and this difference affects their approach to CDM."

For VA, its biggest challenge has been the sheer size of the agency. "VA has approximately 184 Offices of Information Technology throughout the United States, but we have only one network security operations center," says Zeitz. "So, how do we scan the entire VA network, identify flaws, propagate that information across the organization, and repair the flaws—all within the 72 hour timeframe that is CDM's goal? Just deciding where to begin was a challenge for us."

Zeitz says that the guidance he received was to move forward with the discovery work. "Let's install the tools and do the discovery to see what's on the network. That's where we have to begin," Zeitz explains. "I believe we're at CDM Phase 1. We're finding out interesting things we never knew about how data flow on our network. What we're doing now is defining *normal*." When will Zeitz know that his Phase 1 work is complete? "When I can look at something and quickly see whether it's normal or not normal on my network with a reasonable amount of accuracy. Then, I believe we will be there."

Zeitz says that the best way to make the implementation process as smooth as possible is to explain not only *what* is being done but *why*. "We need to keep in mind that we have to implement this program without disrupting the regular quality of our IT services. If people understand that CDM will ultimately improve our quality of service, we'll get that ownership buy-in we need to make it work," Zeitz says.

> *"If people understand that CDM will ultimately improve our quality of service, we'll get that ownership buy-in we need to make it work."*

Maintaining a clear vision while making adjustments using quality data and expert collaboration moves essential enterprise programs in the right direction.

LinkedIn

ALEXANDER KEELY

Senior Lead Technologist and Program Manager, Booz Allen Hamilton

JEREMIAH CLIFTON

Information Security Architect,
Major U.S. city

Jeremiah Clifton is a versatile information security professional with expertise in risk and security program management. His career spans technology and security practitioner roles at NASA and private-sector clients. Jeremiah currently leads program and policy management for one of the largest municipalities in the United States. He is proficient in deploying the NIST Risk Management and Cybersecurity Frameworks to meet FISMA, CIKR, PCI, HIPAA, and privacy regulations and standards. Jeremiah maintains CISSP, CISM, CCSP, GMON and TOGAF 9 certifications.

LinkedIn

The idea behind CDM is not new. Jeremiah Clifton, an information security architect for a major U.S. city, explains that security professionals have long recognized the need for continuous monitoring as part of a risk-based approach to securing their systems and data. "I have always been in favor of continuous monitoring and on-going risk management as a way to supplant compliance strategies that so often dominate federal, state and local approaches to security," Clifton says.

Clifton says that one of the greatest challenges for organizations now implementing CDM is changing their security culture from a compliance focus to a risk-management focus. "Compliance-based security is static," Clifton says.

KEY LESSONS

1. **One great challenge for many organizations now implementing CDM is changing their security culture from a compliance focus to a risk-management focus.**

2. **With CDM, risk management is a business problem, not just an IT security problem.**

"Compliance can create complacency, but CDM forces you to…seek out unusual events and changes taking place in the system, and then make decisions based on how the events and changes affect the risk posture."

The compliance mindset is that if everything is configured according to standards—if you build big walls and keep up with patch management and all the things you are supposed to do—it will keep out the bad guys. "There's something comforting about going through a checklist of security tasks based on testing and evaluations, especially when you are dealing with networks so large it's difficult to know exactly what's on them, and feeling secure because you've checked off all those things," says Clifton. But, too many breaches and systems operating for too long with persistent threats have proven that compliance is not enough.

CDM is a change in mindset for many organizations. "Compliance can create complacency, but CDM forces you to stay active, to become a hunter, to monitor for and seek out unusual events and changes taking place in the system, and then make decisions based on how the events and changes affect the risk posture." This approach requires a much more intensive and granular analysis of networks, and it means acquiring new capabilities. "CDM not only means changing the way you think about threats and risk, but also automating tasks once performed manually. It's impossible to undertake continuous diagnostics and rapid mitigation on huge government networks without tools that automate the process," Clifton says.

Clifton believes that one of the most important steps in successfully implementing CDM is making it a business problem, not just an IT security problem. "I've had the greatest success when I run a full risk assessment with the business side of organizations. When you get finance, legal and the business stakeholders in a room and start talking about risk, they see that thinking in terms of risk is really about looking to the future," Clifton explains. "They become aware of what could happen, and they start asking questions about how they can avoid it." In that context, it then becomes clear why they have to make these baseline assessments of their network; why they must be able to see what's "normal" in the system; and why they need tools that identify anomalies and help them make sound, risk-based decisions about real events happening in real time.

> *"CDM not only means changing the way you think about threats and risk, but also automating tasks once performed manually."*

The biggest challenge that I have seen so far is that people just don't know what's on these networks that CDM tools are being deployed to. This concerns them. It's a risk in that oftentimes, people think they are operating at 100% compliance, but they have not taken into account the devices that are on the fringe—meaning they don't support an endpoint client and they don't allow for scanning of the endpoint for detection. It's been said hundreds of times, but you can't protect what you can't see.

Website | LinkedIn

TIM JONES

Manager of Systems Engineering, ForeScout

STEVEN HERNANDEZ
CISO,
Office of the Inspector General, U.S. Department of Health and Human Services

Steven Hernandez, MBA, CISSP, CSSLP, SSCP, CAP, CISA, HCISPP, ITIL, is the CISO, Director of Information Assurance for the Office of Inspector General at the US Department of Health and Human Services. With over 19 years of progressive information assurance leadership in multiple industries, including international heavy manufacturing, global finance, higher education, and US Federal Government, Hernandez is a sought after leader in risk management and execution. Steven volunteers as a member of (ISC)2's Board of Directors.

Website | LinkedIn

At the U.S. Department of Health and Human Services (HHS), Steven Hernandez, chief information security officer to the HHS Inspector General, says that the tools the DHS has imposed are often robust and the implementers good at what they do. "They know how to do this," he explains. "Initially, everything works great; then, you begin implementation and things start to get a bit wonky."

An example of what Hernandez is referring to is the implementation of an application that, when demonstrated, had tons of capabilities. When implemented, however, federal agencies learn that the CDM program pays only for the initial deployment. "I'm responsible for the rest," says Hernandez. "I have to look at it from a financial perspective and determine whether it makes sense to eliminate those capabilities that are duplicative." He points out that often, his agency has tools in place that do the same job.

KEY LESSONS

1. **When reviewing new applications, be sure that the services shown are the services that will be delivered without additional cost.**

2. **Ensure your infrastructure is sufficient for whatever technologies you plan to implement. The responsibility for improving infrastructure usually falls to the agency.**

> *"Lessons learned from Phase 1: We're making sure that what we bring on board is priced correctly so that it's just what we need in terms of capability."*

"Lessons learned from Phase 1: We're making sure that what we bring on board is priced correctly so that it's just what we need in terms of capability. If it's going to replace something, we have the option to build that functionality out in an economical and time-sensitive fashion."

Hidden costs are another challenge HHS has faced. Hernandez says, "A lot of the CDM project has pretty hefty infrastructure requirements. Depending on where you are and how DHS surveyed you, the underlying infrastructure isn't free and, in many cases, was not included as part of the purchase." He points out that although CDM is billed as being free to federal agencies, "There's no such thing as a free puppy, and some of the care and feeding caught us off guard."

"Moving forward, we've been cautious about the infrastructure requirements for the tools and capabilities. We've pushed back in some cases, and we had some success doing so. Moving into Phase 2, we're making sure that any kind of hidden costs are taken care of," says Hernandez.

The most daunting challenge Hernandez sees now is the future. "CDM as it's designed is a big challenge. There are opportunities here to clarify and strengthen the program, especially in terms of cloud environments." Meanwhile, Hernandez points out that "Those going into the cloud cannot ignore the requirements of CDM. As an agency, you have to know to ask for it upfront from the cloud providers, and you have to know how to ingest it and port it into your environment to make sure that you're measuring it."

"CDM is designed to be part of a program that watches over a treasure trove of data. If we don't extend CDM into all environments, we're doing ourselves a disservice. That's how folks get blindsided and end up explaining to Congress or the press why they had a breach."

"CDM is designed to be part of a program that watches over a treasure trove of data. If we don't extend CDM into all environments, we're doing ourselves a disservice."

In my experience with the U.S. government's CDM program as an integrator, implementation challenges tend to fall into three categories: technical, social or cultural, and contractual. Taken together, these challenges resulted in significant delays in achieving full implementation of CDM requirements, but have in no way shown that those requirements are unachievable or unwarranted. Rather, program rollout could have been more quickly or smoothly achieved had those issues been more fully and effectively appreciated and addressed during project planning.

Website

PATRICK HOWARD

CDM Program Executive, Kratos SecureInfo

JIM PICHE

Homeland Sector Director,
GSA FEDSIM

Jim Piche administers the Federal Systems Integration and Management Center's (FEDSIM) IT, cybersecurity, and professional services projects at the U.S. Department of Homeland Security and its component agencies, most notably, the FEDSIM–DHS partnership for Continuous Diagnostics and Mitigation, which offers state-of-the-art cybersecurity tools and services to government networks. Jim's sector also supports DHS' secure enterprise network systems and the Technology Integration Program at St. Elizabeth's campus, the future home of DHS.

LinkedIn

As Homeland Sector Director for General Services Administration (GSA) Federal Systems Integration and Management Center (FEDSIM), Jim Piche's organization solicits, evaluates, awards, and administers contracts that assist federal agencies in acquiring CDM–related products and services. His role gives him a unique, high-level perspective of how the CDM program is progressing. "We provide staff to administer the contracts and ensure that deliverables conform to standards and invoices are paid on time. As far as choosing which technology an agency needs, that's an agency CIO decision. Determining how much budget is allocated to a particular CDM product or service is a U.S. DHS CDM program decision."

KEY LESSONS

1. **The goal is to establish a solid relationship between an agency and a CDM service provider, and then let them decide on the technology together, downstream of the initial contract award.**

2. **An agency ultimately needs to have control over its cyber defense posture to meet that agency's mission.**

"One challenge is that the information agencies submitted to describe their network architecture and CDM solution requirements was often incomplete."

From a contracting standpoint, CDM Phases 1 and 2 are well underway. Contracts have been awarded for both phases covering 65 federal agencies in the .gov domain. Piche says, "The agencies are in various stages of implementation. Some have deployed CDM sensors across their networks, and are beginning to pilot data gathering. Others are still in the discovery phase."

These early implementation phases have revealed two major process challenges that Piche's organization is already addressing in its next round of contracts.

"One challenge is that the information agencies submitted to describe their network architecture and CDM solution requirements was often incomplete," says Piche. The result was contract changes after a CDM integrator went onsite and discovered that the network was much larger or configured differently than the agency had originally described.

Another problem arose because of the process DHS used: Phase 1 and 2 contracts covered CDM solutions that DHS had evaluated, approved, purchased and essentially handed out to the government agencies. The agencies began to work with the integrator on implementing the solution they had received, only to decide that they preferred a different solution. "This is understandable," explains Piche, "because the agencies ultimately have responsibility for their cyber defense posture to meet their mission." However, the process created contract complications and often left the contracted integrator on the sidelines.

To address these challenges for subsequent phases, Piche's organization is taking a different approach. The goal is to award contracts with less prescriptive solutions. "We're trying to solicit and select highly qualified integrators and enter into long-term, high-value contracts with them so that they can establish a relationship with the agencies they're supporting," says Piche. In Phases 1 and 2, it was more about the solution than it was the integration and the partnership between industry and the agencies. In this next round of contracts, they are taking the opposite approach. Piche says, "We want to establish a solid, well-founded relationship between an agency and a CDM service provider, and then let them decide on the best CDM technology together, downstream of the initial contract award."

> *"We're trying to solicit and select highly qualified integrators and enter into long-term, high-value contracts with them so that they can establish a relationship with the agencies they're supporting."*

How does a government with departments and agencies ranging from tiny to the size of a major corporation secure thousands of IT systems? The answer is DHS's CDM program. Initially derided by many experts, CDM is clearly making progress—albeit more slowly than originally anticipated. As Jenni Taylor, the immixGroup CDM program manager, says of the government-wide CDM process, "If you care about all the systems, you need a thorough program like CDM."

Twitter | Website | LinkedIn

STEVE CHARLES

Co-Founder, immixGroup

MICHELE THOMAS

CISO, Director of IT Compliance,
U.S. Department of Transportation, National Highway Traffic Safety Administration

Michele Thomas is CISO at the U.S. Department of Transportation National Highway Traffic Safety Administration, where she is responsible for the IT compliance program, privacy program, regulatory compliance on all federal IT acquisitions, and capital planning. Prior NHTSA, Michele was CISO for the U.S. Department of Agriculture Animal and Plant Health Inspection Service. She has 20 years of experience in cybersecurity and information assurance in both the public and commercial sectors.

Website | LinkedIn

Foresight and information sharing are key elements of successful CDM activities according to Michele Thomas, CISO and director of IT compliance for the U.S. Department of Transportation National Highway Traffic Safety Administration (NHTSA). Before NHTSA, Thomas was with the U.S. Department of Agriculture (USDA), which is where she began Phase 1 of CDM. "When the legislation passed," she says, "I looked at the list of approved products and noticed that everyone had formed a partnership with one particular hardware asset management solution."

That realization gave Thomas a way to minimize the challenges other organizations face during CDM Phase 1. "I thought, 'I can get ahead of the game. I can contact the product vendor and run a pilot of the software to at least ramp up my staff on what the software is, how it works and how can we use it.'"

KEY LESSONS

1. **Think ahead, and share information with agencies that have already been through what you're facing to find creative, effective ways to prepare for and manage the tasks ahead.**
2. **Plan for each phase as if it were the initial rollout of any technology or capability. That includes budgeting, personnel and training to ensure that all users understand what's coming and how it will affect them.**

> *"I can get ahead of the game. I can contact the product vendor and run a pilot of the software to at least ramp up my staff on what the software is, how it works and how can we use it."*

The idea worked. The pilot gave her staff time to learn how to use the application so when USDA officially announced its CDM kickoff, Thomas' team was ready. She then shared her knowledge and the team's experience within and outside USDA.

Thomas' experience with the solution paid dividends during the recent WannaCry ransomware threat. "We were prepared for it because we had a handle on our system inventory, we were up to date on our patching, and I knew that when I came into the office on Monday I would have to report my team's status to management. We triple-checked patching to ensure that all our systems were as protected and secure as possible. Then, I made sure that all the other systems administrators were informed and had the tools they needed to protect their systems."

Although Thomas changed agencies before USDA's CDM rollout was complete, she notes that the tasks are the same regardless of agency. "The challenges are knowing what you have, knowing how to use it and using it effectively. So, when the Office of Management and Budget knocks on your door asking for your quarterly numbers, if you've deployed Phase 1 and have the tools in production, you should be able to log in, click a button and get a snapshot of your numbers in real time."

That level of preparation doesn't happen overnight. Thomas suggests starting small. "Choosing your rollout schedule and methodology is critical. The solutions we selected had been on the market for a while. The challenge was integrating them and fulfilling the legislation's requirements. Planning for, configuring, training for, and assimilating all that into your agency's budget and IT strategy is no small thing: It requires leadership that operates with foresight. CDM tools aren't just cybersecurity or IT solutions: They affect financial, business—a lot of things. CDM tools enable business."

"CDM tools aren't just cyber-security or IT solutions: They affect financial, business—a lot of things. CDM tools enable business."

CDM is a fascinating program that has allowed many to adopt and deploy modern commercial technologies. Although there have been many successes, some aspects of the program are limited by constrained product choices. Also, the program has been oversubscribed, thus limiting its ability to deliver timely solutions to all in need. Overall, CDM is a great step toward modernizing and rapidly acquiring commercial capabilities; its successes should be built on and its few weaknesses overcome.

Website | LinkedIn

RONALD NIELSON

Owner, Sharkoptics LLC

FOCUS ON THE FUTURE TO ACHIEVE CDM SUCCESS

JOSH CANARY

Partner,
Touchstone Technology, LLC

Josh Canary brings 20 years of leadership in technology to help clients implement cybersecurity and information sharing best practices. Previously the CDM program manager for CSC, and then CSRA, Josh led programs spanning the homeland security enterprise. Prior to joining CSC, he spent 10 years deploying large technology programs for Global 1,000 companies, including Tier-1 Internet service providers and in manufacturing, financial interests and large retail operations. He holds a bachelor's degree from Georgetown University.

Twitter | LinkedIn

About CDM, Josh Canary, a partner with Touchstone Technology, says, "Try not to get wrapped up in the churn"—that is, the confusion that typically arises as agencies implement CDM. Canary warns that agencies "might miss out on the opportunity to take advantage of the funding that the U.S. DHS has put together as they move into Phase 3."

One problem stems from a lack of capability from DHS. "Currently, there is not enough scope for tasks that would take some weight off the agencies," Canary says. "The rigor of good program management and an understanding of the mission priorities help you scope what can realistically occur with your current staff. For example, do you have management buy-in? Can you get more funding if you need it?"

KEY LESSONS

1. **The noise generated during the rollout of CDM can be overwhelming. Success results from ignoring that noise and applying solid project management skills to each CDM phase.**

2. **CDM is a long-term project, and viewing the activities, processes and strategies for achieving success through a long-term lens reduces confusion and clarifies the necessary steps.**

"They set a reachable goal. They are well organized in terms of what they're trying to do and whom they support...It's not sexy, but a successful Phase 1 can lead to 'cyber hygiene.'"

FOCUS ON THE FUTURE TO ACHIEVE CDM SUCCESS

Canary offers a suggestion for overcoming the confusion. "Relentlessly focus on the mission. You can be distracted by the sheer number of projects available—the number of meetings, conferences, demonstrations and innovations. But, the people who have successfully implemented CDM are those who scope precisely what they're trying to accomplish and stick to their plan."

"Successful CDM implementers have a plan of action and milestones," Canary explains. "They set a reachable goal. They are well organized in terms of what they're trying to do and whom they support, and they're able to bring together stakeholders and then successfully deploy CDM. It's not sexy, but a successful Phase 1 can lead to 'cyber hygiene.'"

"If you look at it from the original charter, DHS designed CDM to bring federal government agencies up to a baseline from which they can then begin to protect their cyber infrastructure." Canary says that agencies should look at CDM as a long-term project, each phase of which is one step toward the longer-term goal.

Canary also points out that CDM came out at the same time as the Federal Information Technology Acquisition Reform (FITARA) program. The result of the two pieces of legislation is "a significant policy shift among the roles of the chief information security officer, the chief information officer (CIO) and the role of DHS. FITARA allows the CIO to tell subordinate agencies what they're going to do in a direct way. CDM allows DHS to say, 'Here are the standards you have to meet.'"

Canary sees this change in relationships as significant because it promotes a different dynamic that can both create confusion, but also help agencies successfully implement CDM. "That dynamic change in relationship can lead to confusion and chaos if roles and responsibilities aren't well defined in advance. Another suggestion is to select an organization within the agency to act as a coordinator for the entire deployment. Getting an organization within the agency to act with DHS, be onsite and know the leadership and management changes—has significantly helped some agencies stay on target, reduce scope creep and stay on schedule."

> *"FITARA allows the CIO to tell subordinate agencies what they're going to do in a direct way. CDM allows DHS to say, 'Here are the standards you have to meet.'"*

Like the NIST framework, the CDM program takes a risk-based approach to cybersecurity, which separates it from prior federal programs that put evaluation mechanisms like agency report cards ahead of evaluating risk (which should be the first step agencies take to understand their security posture). Eligible agencies and organizations should take advantage of the special CDM pricing to acquire tools that, among other things, allow continuous network monitoring to identify vulnerabilities and reduce risk.

Twitter | Website | LinkedIn

JAMES HAYES

Vice President, Government Affairs, Tenable

ISMAEL VALENZUELA

Principal Engineer,
McAfee

As principal engineer at McAfee and a Certified SANS Instructor, Ismael Valenzuela specializes in incident response, security operations centers, forensics, malware analysis and threat research. A top cybersecurity expert with a strong technical background, Ismael has provided security consultancy and guidance to large government and private organizations, including major European Union institutions and U.S. government agencies. Ismael holds a bachelor's degree in computer science, as well as numerous professional certifications, including the highly regarded GIAC Security Expert.

Twitter | Website | Blog | LinkedIn

The focus of Phase 1 of the the U.S. Department of Homeland Security's CDM program is on baselining networks and identifying vulnerabilities. This is important work, says Ismael Valenzuela, senior director and principle engineer at Foundstone Consulting, a practice within McAfee Professional Services. But, he also sees a need to move toward more aggressive threat identification as soon as possible. "In its early phase, CDM is focused on discovering, prioritizing and fixing vulnerabilities. That's great: It's basic security hygiene," says Valenzuela. "But, it's not enough to see that some unusual event is occurring in the network. You also need to understand *why* that event is occurring."

KEY LESSONS

1. **Baselining networks and identifying vulnerabilities are important tasks, but organizations need to move toward more aggressive threat identification as soon as possible.**

2. **Organizations must use technology to automate as many tasks as possible, but you also need that skilled analyst who understands why the issue is taking place.**

> *"It's not enough to see that some unusual event is occurring in the network. You also need to understand why that event is occurring."*

To do that, Valenzuela points out one of the great challenges organizations face as they move forward with their CDM implementations. "You need a new level of understanding to interpret all the data coming from the many sensors generating vast amounts of new data about vulnerabilities and anomalies in the network," he explains. "People are scanning for things that are known, such as a patch or something bad that you know shouldn't be there. But, what about looking for the presence of threats for which there might be no known signature?"

Not only are there more data to analyze than ever before, but it's also necessary to look deeper into those data to discover what is truly a threat. That deeper dive means that security organizations can quickly become overwhelmed by the new flood of incident data, and all they can do is address those incidents without looking deeper to determine whether a more persistent threat is at work. "They are spending so much time putting out fires they can't see what's behind them," Valenzuela explains. "Success requires using technology to automate the task as much as possible, but you also need a skilled analyst who understands why the issue is happening." Ideally, subsequent phases of CDM implementation will include an emphasis on enabling organizations to build the security analyst skills they need to go beyond simply responding to the larger volume of incidents they're discovering so that they can proactively hunt for threats. "If you're spending a lot of time looking for a Trojan here or a worm there, you aren't looking at the elephant in the room because you don't even know what that elephant looks like. Once you know what it looks like, then you can search for it on your network."

As organizations move beyond the early phases of CDM implementation, Valenzuela recommends that they acquire the skills to get past simply monitoring and remediating vulnerabilities. "My advice is to focus on the threats—more specifically, the threats that are most applicable to your industry."

"My advice is to focus on the threats—more specifically, the threats that are most applicable to your industry."

The CDM program requires incredible precision—rightfully so, given its important mission. One challenge has been adding new products to the BPA. We've overcome this stumbling block by implementing a detail-oriented process to make sure we're providing accurate and complete information to our CDM CTA partners—a process that DHS will ultimately review. We've also hosted multiple CDM Speed Networking events to inform our cybersecurity vendors of the significance of the CDM program and the importance of accuracy with their CDM submissions.

Twitter | Website | LinkedIn

JENNI TAYLOR

Contracts Program Manager, immixGroup

Mighty Guides

Mighty Guides make you stronger.

These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you. Reading a Mighty Guide is kind of like having your own team of experts. Each heartfelt and sincere piece of advice in this guide sits right next to the contributor's name, biography, and links so that you can learn more about their work. This background information gives you the proper context for each expert's independent perspective.

Credible advice from top experts helps you make strong decisions. Strong decisions make you mighty.

 I 62 Nassau Drive I Great Neck, NY 11021 I 516-360-2622

www.mightyguides.com

tenable™

CDM Compliance...And So Much More.

Maximize **Your Security Posture** with Tenable.

Learn more about using security frameworks to protect critical systems and data.

tenable.com