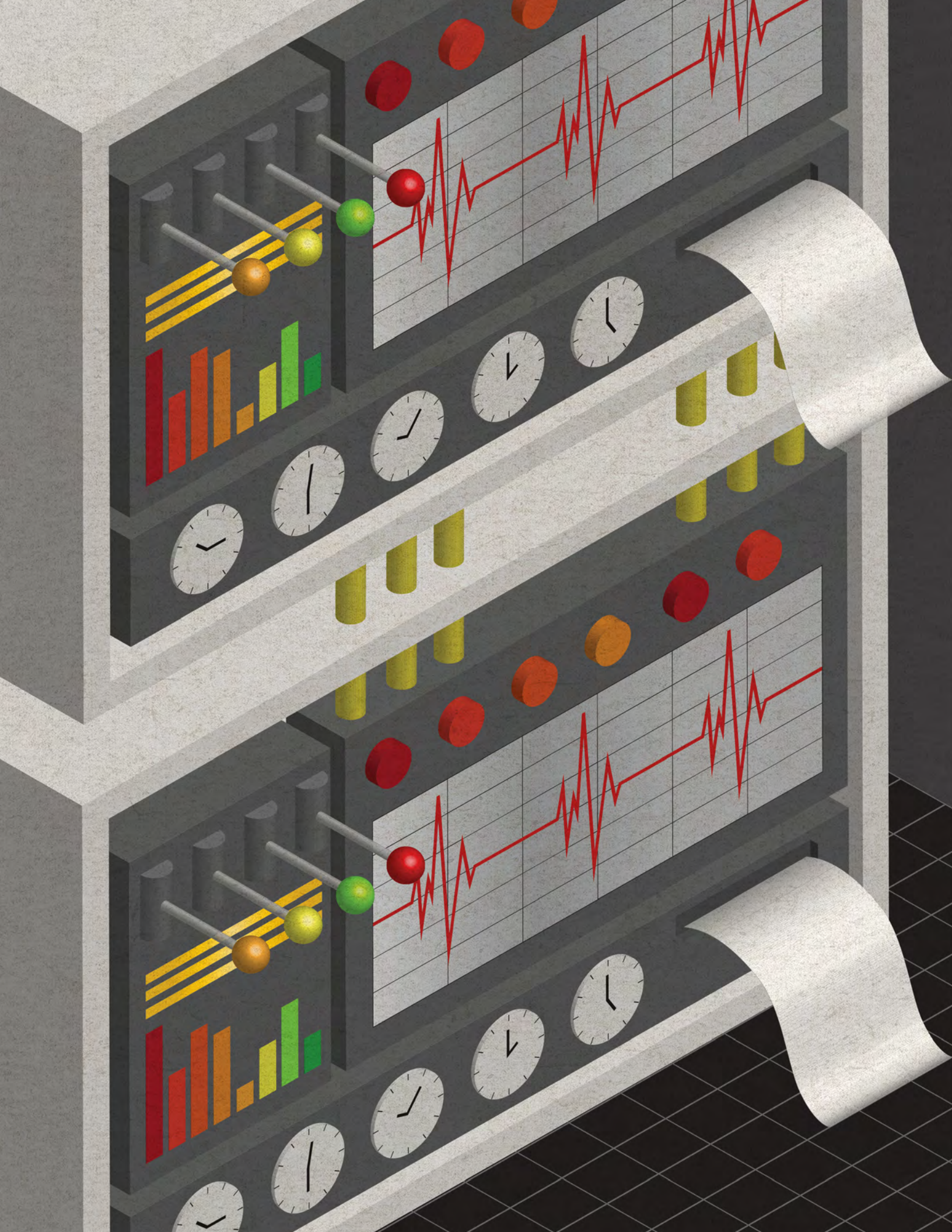
THE CONTINUOUS DIAGNOSTIC & MITIGATION PROGRAM FIELD GUIDE



EXECUTIVE SUMMARY

Cybersecurity is a preeminent concern for government officials. In today's world, it's imperative that government protects our critical infrastructure to preserve our physical and economic security. To do so, cyber professionals must obtain real-time visibility of networks, improve ability to mitigate known flaws and decrease security risks by reducing their vulnerabilities.

That's why the Continuous Diagnostic and Mitigation (CDM) program, which enables government entities to decrease known cyber risks and flaws by expanding their continuous diagnostic capabilities, is so important. CDM is poised to have a tremendous effect on government by changing the way agencies combat cyberthreats and improve cybersecurity preparedness. The program does this by:

- *Strategically sourcing tools and continuous-monitoring-as-a-service (CMaaS) solutions.*
- *Improving visibility of network vulnerabilities, risks and flaws.*
- *Mitigating and identifying flaws at near-network speed.*
- *Supporting efforts to provide adequate, risk-based and cost-effective security solutions.*

CDM will help agencies procure commercial continuous monitoring solutions. First, the Homeland Security Department, which established the program, will help an agency set up the proper sensors to conduct an automated search for cyber flaws. The results will feed into a local dashboard and export customized reports. The reports can then alert network managers to the most critical flaws and risks based on weighted scores. Administrators will receive prioritized alerts to help allocate resources to mitigate flaws. Finally, progress will be tracked through dashboards and can be compared among department and agency networks, which will help improve the shared risk of each department.

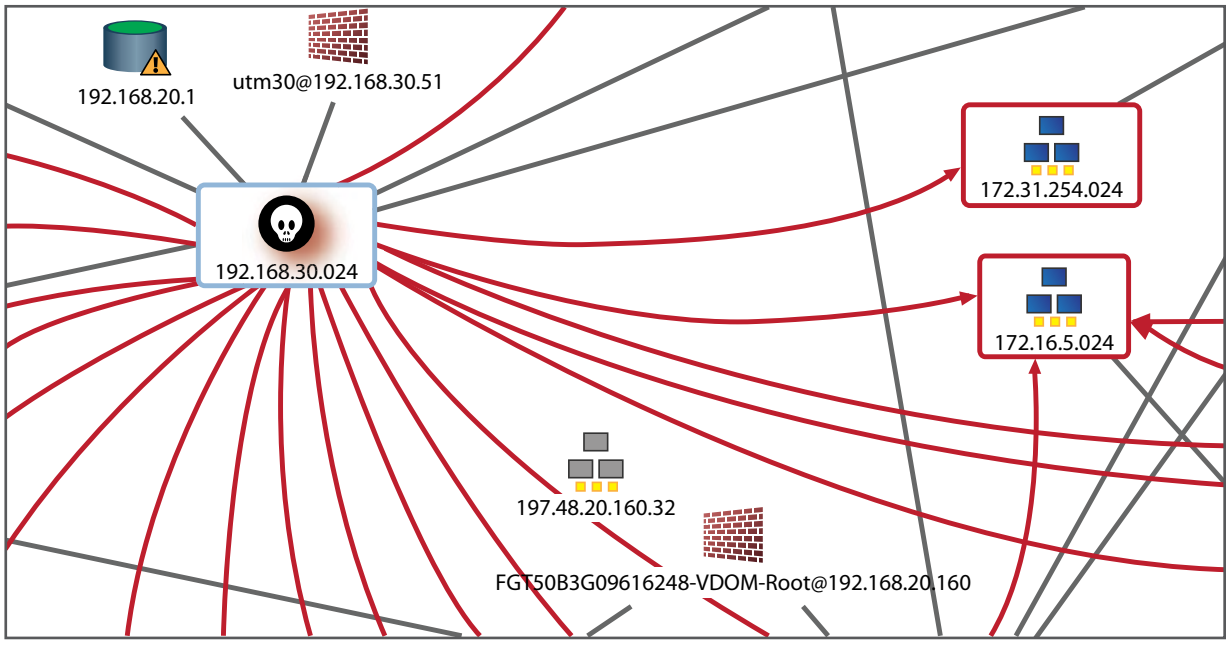
Although new technology continues to enter the marketplace to make life easier, it also leads to increased security risks. Technology trends such as the Internet of Things, mobile and cloud computing have helped meet the public sector's growing and multifaceted needs. At the same time, this dynamic has led to conflicting interests and added complexity. On one hand, agencies must leverage new technology to meet demand. On the other, technology must be deployed safely and securely to protect data and confidential information.

Government needs to become more agile and efficient in the way it combats cyberthreats. CDM is a step in the right direction. Explore our guide to learn more.

CONTENTS

Automate 2 Key DHS CDM Requirements

security device management and vulnerability risk analysis



Manual processes are failing to keep attackers out

The New DHS Continuous Diagnostics and Mitigation (CDM) program is automating agency cyber defenses to help decision makers assess real time cyber-attack readiness and implement effective responses with current staff levels.

FireMon's Security Intelligence Platform automates security device management and vulnerability risk analysis by continuous monitoring and managing changes in overall security posture – keeping the bad guys out.

To learn more contact us at fedgov@firemon.com
or visit www.firemon.com/solutions

FIREMON

PROACTIVE SECURITY INTELLIGENCE

WHY REAL-TIME AWARENESS IS ESSENTIAL TO YOUR CYBER PROGRAM

Tim Woods, Vice President of Customer Technical Services, FireMon, provides his insights on the CDM program and the impact it will have on government.

What do agencies need to know as a starting point for CDM?

Agencies need to know, or at least they need to have a good idea of where their biggest weaknesses are today and how that maps to the functional areas within the CDM program. Obviously CDM covers a number of different areas, 15 functional areas, and you can't really go and attack all of them at once. So there is a bit of an assessment or strategic planning that an agency has to put itself through. Everybody is trying to do more with less, and the government is no different.

Can you talk a bit more about your Security Intelligence Platform? Why is this an important element to a cyber solution?

FireMon's security intelligent platform provides significant value across many of the key CDM functional areas. Most importantly, it's real time. We always have been real time. We provide real time visibility into changes as change happens. So it's real time situational awareness and a level of visibility that's missing from many security architectures today. I frequently have security professionals tell me that they are not confident in security being provided by their selected enforcement technologies. And it's in no way a reflection on the quality of the products that they've selected in the past, but rather the lack of visibility they have into the operational effectiveness of their device's configurations and policies.

Do we need to stop before we do anything else and go and remediate that potential exploitation point or, based on the needs of the business for access to information, is that an acceptable risk? The FireMon platform can actually empower security administrators to conduct security related tasks through automation that they just haven't had the time to do in the past, essentially giving them back time in their day."

Can you talk about compliance and security? Does CDM help you get the best of both worlds?

Compliant doesn't necessarily mean secure. It is a continuous effort that has to take place. Being compliance takes a significant effort to achieve compliance and to stay there once you get there. But I think automation is key. Again it comes back being able to have the technical resources and enough time in the day to do the things they know they have to be doing.

Without [automation], because of the number and size of policies, and I'm not just talking about firewalls, I'm talking about routers and switches and load balancers and all the different key security technology that are deployed today, [administrators] need to have the ability to analyze how those policies behave, and this cannot be done in a manual fashion anymore, you just miss too much detail. So we need some type of automated way to understand what the behavior of the defenses is supposed to be, are we in compliance, and when, and when we go out of compliance, we need to understand that and ideally be automatically. Without the right technology and the ability to gain visibility into the operational effectiveness of our policies, it's impossible to earn and maintain compliance.

By following Woods' insights, your agency can improve cybersecurity efforts through much-needed visibility and real-time awareness of your defensive posture to help your teams combat threats.

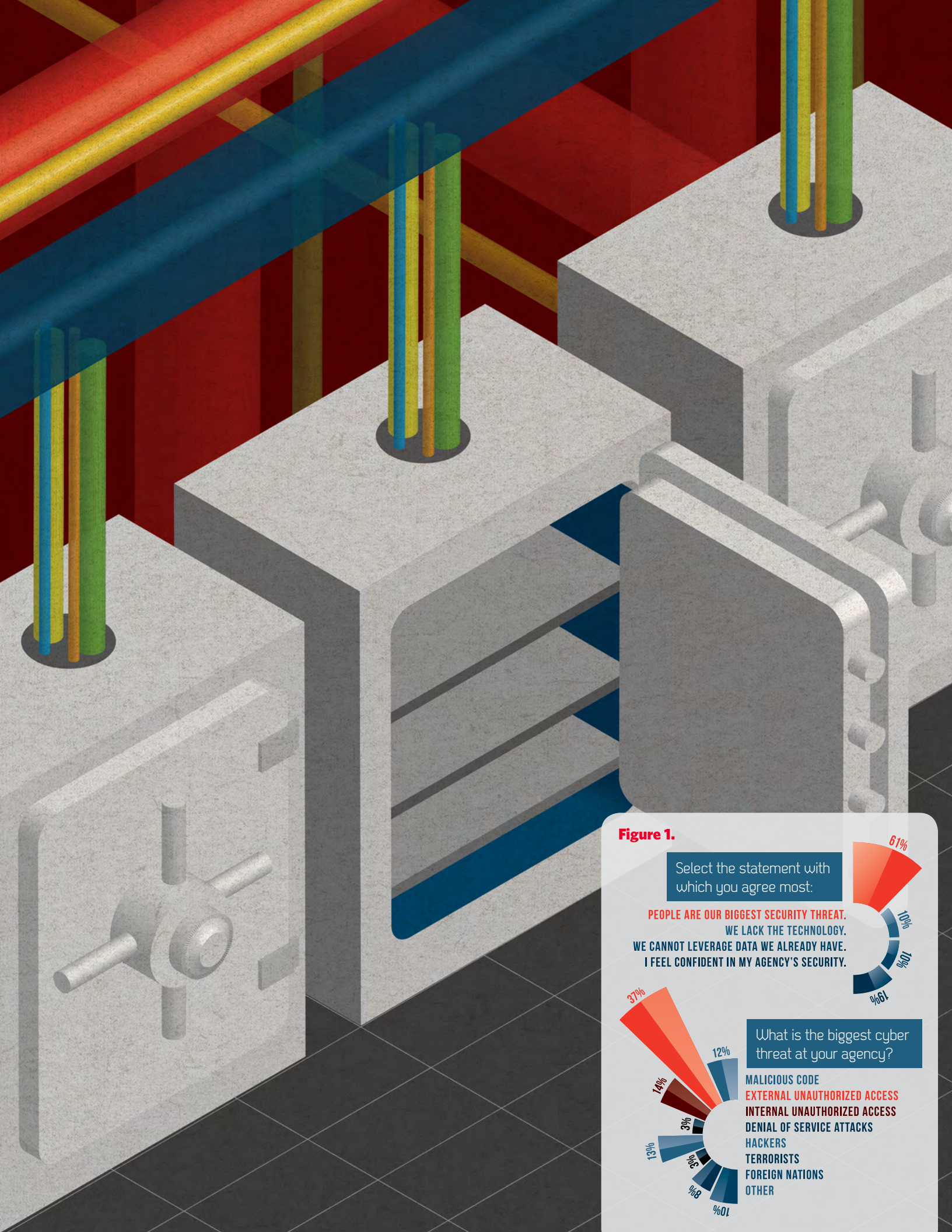


Figure 1.

Select the statement with which you agree most:

PEOPLE ARE OUR BIGGEST SECURITY THREAT.
WE LACK THE TECHNOLOGY.
WE CANNOT LEVERAGE DATA WE ALREADY HAVE.
I FEEL CONFIDENT IN MY AGENCY'S SECURITY.

What is the biggest cyber threat at your agency?

MALICIOUS CODE
EXTERNAL UNAUTHORIZED ACCESS
INTERNAL UNAUTHORIZED ACCESS
DENIAL OF SERVICE ATTACKS
HACKERS
TERRORISTS
FOREIGN NATIONS
OTHER

DEFINING WHAT IT MEANS TO BE SECURE

What does it mean to be secure? We wanted to know how an agency's information technology officials could say with confidence that they have taken the right steps to protect its information. It became quite clear that security is not only a state of being, it's also a mind-set and the ability to create a culture rooted in security. In the dynamic and asymmetric world in which cyber professionals operate, they must constantly look at innovative ways to stay ahead of attackers.

Through our research and with help from industry experts, we identified five dominant themes about what it means to be secure.

❶ Having Real-Time Awareness

Attacks on agencies are occurring more frequently than ever, and agencies now must be able to analyze threats and attacks in real time. Being secure doesn't just mean being able to respond quickly; it's having the knowledge and insights to spot attacks as they are unfolding. To gain that awareness, agencies must understand what their network looks like and who accesses it and how.

"The reality is most organizations don't know what being totally secure looks like in the cyber world," said Robert Roy, federal chief technology officer at HP Enterprise Security Products. ow can they if they don't know what they are protecting, or they don't understand the vulnerabilities, or they don't fully understand the threat? Any secretary should be asking: 'How secure is my business?' and to answer that question, it is going to take a fully implemented CDM solution, both technically and organizationally."

❷ Continuous Assessing Vulnerabilities

You could craft the best plans and policies, but they will fall flat if the policies are not enforced. A risk management policy should help you understand who access data, how they access it and when. The policy will also provide clarity on proper data usage for stakeholders and data users.

"Enforcing a dynamic cybersecurity risk management policy is crucial to being secure. This policy needs to be thoroughly understood and adopted by all stakeholders, both internal and external—those accessing your data, your network, and your resources. This policy cannot be stagnant; it must adapt to evolving threats to the network. It should enable risk-based decision-making, aligned to your mission and business objectives. Your users will always be the weakest link in the chain, so it's essential that all levels of the workforce participate in continuous cybersecurity education in order to understand the risk they pose as users of the network, and how they can eliminate those risks," said Chris Wilkinson, director, Cybersecurity Technologies, immixGroup.

❸ Mitigation and Administering Rapid Response

In today's environment, organizations must quickly deploy mitigation techniques and respond rapidly to complex attacks. For government, this means that there needs to be a way to connect people to technology.

"Being secure is a moving target insofar as you have to understand the cybersecurity is ever evolving," said Patrick Flynn, director of Homeland/National Security Programs at Intel Security Federal Business Development. "It's like asymmetric warfare in Afghanistan or Iraq – you don't know what the enemy necessarily looks like. So as long as you understand that, and you have the ability to put the solutions in place and bring in the human to understand and recognize those threats."

❹ Gaining Clarity from Complexity

There is no doubt that security is complex for government administrators. In our survey of 160 cybersecurity professionals, we found that the biggest cyberthreats agencies face are external unauthorized access and people. (See Figure 1.) Respondents believe their largest gaps in cybersecurity solutions reside in least privilege and infrastructure integrity (people and devices). These findings show that CDM is positioned well to provide access to the government community to the right solutions to improve their overall security posture.

These various attack vectors are challenging cyber professionals. "One of the biggest challenges faced by both government and commercial enterprises today is that of rapidly growing complexity," said Tim Woods, vice president of engineering at FireMon."I'm not referring to the type of complexity that one finds in a well-orchestrated security architecture, but moreover the unnecessary complexity that has crept in over time that has left us with large gaps in our security defenses. Unnecessary complexity gives rise to the probability of human error creeping into the equation as well."

❺ Automating Processes

Automation is an imperative part of cyber defense. By automating traditionally manual processes, agencies can improve compliance and reporting strategies. Automation can help IT managers react quickly and develop new ways of thinking about cyber issues.

Still, no defense strategy is flawless; some attacks are bound to work. Cybersecurity today is as much a practice of damage control as it is of prevention.

"Today's real world requires a threat-centric approach to security. We have to assume that a certain number of attacks are going to be successful," said Steve Caimi, industry solutions specialist at Sourcefire, which Cisco acquired last year. "We need to have the capabilities to know that it's happening right now and react quickly."

For cybersecurity professionals, defining what it means to be secure is complex. CDM helps because it's designed to improve agencies' security posture by assessing, analyzing and mitigating attacks.

As we explore how to participate in the CDM program, it's important to keep these considerations of an effective cybersecurity policy in mind.

Better security, better networks.

No more playing catch up. Get ahead of future threats. It's time to think like a bad guy. Your network is evolving to meet mission requirements and CDM directives, but security is a big concern. HP Enterprise Security Products knows what you're up against and we have the scale and deep domain expertise to predict and disrupt threats before damage is done, protecting every part of your enterprise. Our comprehensive, integrated and easy-to-deploy security products help you meet your agency's goals – on time and on budget, so you get to threats before they get to you.

Learn how to better disrupt threats or mitigate their severity at HP Protect 2014. Visit **hpprotect.com**.

Make it matter.

RETHINKING YOUR CYBERSECURITY APPROACH: IS CDM RIGHT FOR YOU?

To learn how HP is helping government agencies participate in the Continuous Diagnostics and Mitigation (CDM) program, we spoke with Robert Roy, CISSP, CEH, Federal Chief Technology Officer, HP Enterprise Security Products (ESP).

What kind of opportunities does the CDM program present for government?

We see several key opportunities that the CDM program presents for government. First, they have a program. The program comes with vetted technologies and service companies that are standing by to fulfill the CDM requirements that move the government to combatting threats in real time. I can't recall a single security program of this magnitude that has so many technology and service companies lining up their resources with such focus and determination.

Second, they have a timeline. When you give people a plan and tell them when to execute it, more often than not you are setting them up for success.

And finally, but perhaps most importantly, there is money. Having the best plans and timelines doesn't mean a thing without funding. By providing a centralized pool of funding, both government and the blanket purchase agreement (BPA) contract holders can benefit from centrally coordinated and leveraged buying by getting the best pricing and reducing the number of individual contracts. This cuts down on waste and enables the government to achieve the best possible pricing scenarios.

CDM covers 15 continuous diagnostic capabilities during three separate phases. Our report identifies each phase and the 15 functional areas. Could you provide some additional context as to the best way to approach the 15 functional areas?

I think every organization is going to approach the 15 functional areas differently based on their internal structure, current state and priorities. As John Streufert, director of Federal Network Resilience at the Department of Homeland Security, recently commented at a government event, we've all been doing the individual functions for the last 20 years, and now we're just bringing it all together for a common security goal.

We like to think of the 15 functional areas spread across four primary IT domains: configuration, access, vulnerability and event management. All of the CDM BPA holders and technology providers can map their solutions into this simplified framework, which enables a more relevant discussion with a government customer since they can focus their resources into one of these domains.

How can HP help agencies as they participate in the CDM program?

HP representatives have been supporting the cybersecurity requirements of the federal government for over a decade. The introduction of CDM has helped us to understand how we can better deliver products and services for the federal mission in a consistent and useful way. The program actually makes it easier to understand government priorities, and since we know both the program and all of the contacts to get the work done, we can help agencies prioritize their current needs according to the timelines established by the program.

What are some best practices for the government community to get started with CDM?

- *Use what you own, and use it better. We see many organizations using only a fraction of their technology investments.*
- *Collaborate on threats in real-time with your peers. Experience has shown that effective attacks are immediately shared by the assailants, but the victims often wait weeks to publish a successful attack to a website or send details via email. HP Threat Central was designed specifically to address this problem.*
- *Learn, learn, learn. Attend courses, training and security events. HP offers workshops, training and assessments to help improve your security capabilities.*
- *Architecture matters. Get in front of your security challenges. The right architecture can help move your security from purely reactive to proactive – stopping threats in their tracks.*

By following these best practices, and taking a hard look at your organizations readiness level, you'll be well on your way to a safer and more secure government agency.


VIRUS

A HISTORY OF RISK-BASED & COST-EFFECTIVE CYBER POLICY

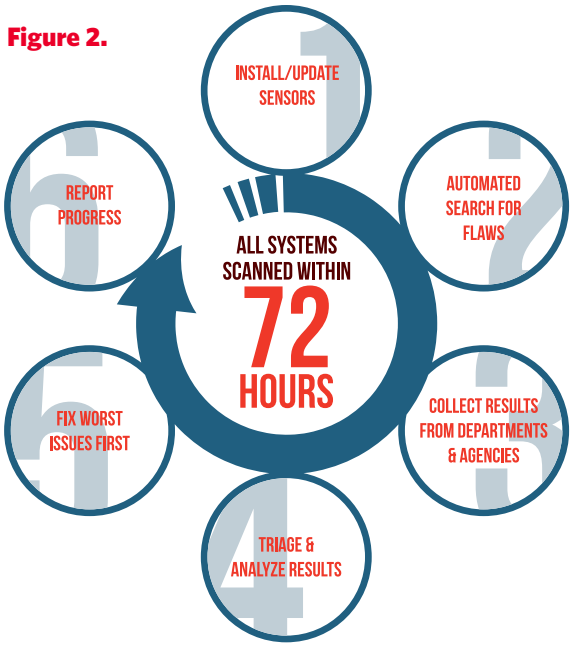
As our systems have become more interconnected and diverse, risks for cyberattacks have increased. In response, DHS has established the CDM program, which is looking to drastically improve the way agencies monitor, assess and mitigate cyberattacks.

The program will enable government officials to gain increased visibility of their networks and understand how to improve their overall cybersecurity efforts. The image in Figure 2 (data from DHS) shows how the program will work. Additionally, CDM:

- *Installs sensors to search and scan for known cyber flaws.*
- *Measures results of known threats, which are then placed into a local dashboard to customize reports.*
- *Allows network managers to see their worst cyber risks, which are based on standardized and weighted risk scores, and notifies them if immediate action is needed.*
- *Provides agencies the ability to allocate limited resources based on risk levels.*
- *Tracks progress and allows information to be shared among agencies to compare assessment levels.*
- *Creates three phases of deployment and 15 critical controls and three phases of deployment.* *(See Page 8.)*

CDM builds on a long line of policies and mandates that support the need for a risk-based policy for cost-effective control for government networks. As early as 1995, with the passage of the Paperwork Reduction Act and the Clinger-Cohen Act, Congress mandated policies for effective controls to mitigate risks. In 2000, the Office of Management and Budget released Circular A-130, Appendix III, "Security of Federal Automated Information Resources," which required executive-level agencies to:

Figure 2.



CDM TIMELINE

1995

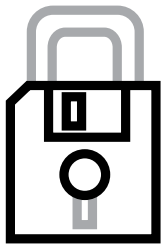
Congress mandated policies for effective controls to mitigate risks with the passage of the Paperwork Reduction Act and the Clinger-Cohen Act.

- *Assign officials to security responsibilities.*
- *Periodically review security controls in their information systems.*
- *Authorize systems prior to and periodically during operations.*
- *Create a plan for security.*

Circular A-130 was a precursor to the Federal Information Security Management Act (FISMA) of 2002. It asked agencies to explore methods to create a cost-effective and risk-based cybersecurity program.

In 2003, to meet FISMA requirements and improve the agency's security, John Streufert, now director of federal network resilience at DHS, began to lay the groundwork of a continuous monitoring solution, which would ultimately evolve into the CDM program.

2000



The Office of Management and Budget released Circular A-130, Appendix III, "Security of Federal Automated Information Resources."

"We began a practice of what was called then, and is referred to informally now, as continuous monitoring, where we would go through some of the checks that used to be done once every three years with a frequency of at least every three days," Streufert said.

Although FISMA was a step in the right direction, it couldn't keep pace with today's environment. Understanding this, Sen. Thomas Carper (D-Del.) in 2009 called for the creation of improved methods to track expenditures related to cybersecurity in testimony to the Senate Homeland Security and Governmental Affairs Committee, which he now chairs. At the time, he was chairman of the committee's Federal Financial Management, Government Information, Federal Services and International Security Subcommittee..

2002

Federal Information Security Management Act (FISMA) asked agencies to explore methods to create a cost-effective and risk-based cybersecurity program.

Carper highlighted Streufert's work at the State Department, where Streufert had been chief information security officer and deputy chief information officer for information assurance, and how continuously monitoring systems had led to cost savings and reduced risk by 90 percent. This testimony was an early indication of formalizing the CDM program, and placing Streufert and DHS as the key leads for it.

"So now moving forward to the 2014 timeframe, there are proposals that the Continuous Diagnostics and Mitigation program funded by DHS would buy a set of sensors and supply specialized labor to assist the civilian government agencies in automating their security testing in a way that used to be done manually," Streufert said.

But to capitalize on the automation techniques cyber experts touted, the program

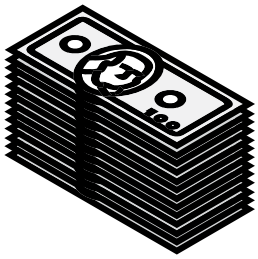
2003

John Streufert, now director of federal network resilience at DHS, began to lay the groundwork of a continuous monitoring solution, which would ultimately evolve into the CDM program (to meet FISMA requirements and improve the agency's security).

"We began a practice of what was called then, and is referred to informally now, as continuous monitoring, where we would go through some of the checks that used to be done once every three years with a frequency of at least every three days," Streufert said.

Continuously monitoring systems had led to cost savings and reduced risk by 90 percent. This testimony was an early indication of formalizing the CDM program, and placing Streufert and DHS as the key leads for it.

Sen. Thomas Carper (D-Del.) called for the creation of improved methods to track expenditures related to cybersecurity in testimony to the Senate Homeland Security and Governmental Affairs Committee, which he now chairs.



CDM continues to build momentum across dot-gov networks. DHS is already in agreement with 108 of 124 dot-gov organizations to deploy CMaaS solutions.

2009

CDM!

2012

DHS began to put together budget proposals that were ultimately funded at $185 million for 2013.

NOW

This led to DHS' becoming responsible for the development of the contracts and the proposed operation of the diagnostic testing capabilities and maintenance of a central dashboard to collect agencies' status.

needed a central authority. In 2012, DHS began to put together budget proposals that were ultimately funded at $185 million for 2013.

"That funded program turned into a series of contracts, called the continuous-monitoring-as-a-service (CMaaS) contract, and a companion acquisition vehicle to purchase a dashboard where the output of the data centers and the results of the security testing get posted, so that the departments and agencies can then use the information to strengthen their cybersecurity posture," Streufert said.

From the very early stages of the program, there was a proposed division of labor between DHS and partnering agencies. As CDM became formalized, Congress realized that if each agency developed its own methods of cybersecurity, they would be more expensive, and potentially less effective, than if a central authority managed cyber programs.

This led to DHS' becoming responsible for the development of the contracts and the proposed operation of the diagnostic testing capabilities and maintenance of a central dashboard to collect agencies' status. The responsibility of the actual mitigation and repairs from known cyber flaws, which are realized by CMaaS solutions, remains with each agency.

CDM continues to build momentum across dot-gov networks. DHS is already in agreement with 108 of 124 dot-gov organizations to deploy CMaaS solutions. Streufert notes that agencies will have to look at strategic sourcing as a means to truly take advantage of the program, and then work to measure the effectiveness of each program to be sure agencies are yielding the highest possible return.

CDM comes at an important time. The difference between now and the early 2000s is that agencies can no longer react in weeks or months; they must act in minutes to combat attacks because of their diversity and sophistication. Additionally, when you look at cyber issues, a shared risk has developed. Not only do officials need to think about security at their agencies, they also must be cognizant that systems, information and data often are interconnected in a way that requires a new – and more dynamic – way of thinking about cybersecurity.

HOW RESILIENT ARE YOUR CYBER DEFENSES?

To protect your systems against threats from within your agency and around the world, you need rapid, reliable access to the strongest tools available --- and the expertise to help you choose the right solutions.

As a supplier for more than 70 top cyber security technology vendors, immixGroup offers the IT products you need through the contracts and business partners you prefer. And our Trusted Supplier Program protects you from the risk of sourcing counterfeit products.

www.immixgroup.com/Cybersecurity ▪ 703.752.0610

immixGroup
Cybersecurity Technologies

INDUSTRY'S ROLE TO SUPPORT CDM: HOW TO GET ENGAGED

Chris Wilkinson, Director, Cybersecurity Technologies, immixGroup, shared with us how immixGroup can help the vendor community and prime contract winners excel with CDM, and remain compliant to help improve government's security posture.

How can immixGroup help Prime Contract holders participate in CDM?

immixGroup has strong relationships with key manufacturers of Commercial Off-The-Shelf (COTS) technology and products that help the prime contract holders create a competitive cybersecurity solution, addressing each CDM functional area. immixGroup has hosted a number of strategic events, on-site meetings, and networking opportunities to facilitate dialogue between the COTS technology vendor community and the CDM prime contractors, providing a unique opportunity to introduce CDM prime contractors to emerging technologies and capabilities. We then help them align those COTS products strategically to the functional areas, and assist in identifying additional capabilities that may fill gaps in some of the functional areas that they may not have addressed in support of their CDM strategy.

How does immixGroup help the vendor community participate in CDM?

We help companies in the vendor community to position themselves to win task orders as a sub to the prime contractor. immixGroup is uniquely positioned to introduce technology manufacturers to the prime contract awardees for consideration in select functions of the primes' CDM solution. We also ensure compliance and work with GSA to strategically add new COTS capabilities as needed to provide the primes with the access to emerging capabilities.

What are some best practices for Prime Contract holders?

Prime contractors really need to fully read and understand the CDM initiative and stay current with CDM, particularly as the program matures and future phases and requirements continue to take shape. They need to identify early the strategic COTS technologies that fulfill each specific functional area, as it could be that the product may needs to be added to a GSA schedule to ensure CDM compliance. Adding a product to the GSA contract vehicle follows a very specific process, and that takes time. So it's important that the Primes build in that time to ensure they can position competitive solutions that are compliant with CDM.

What best practices would you recommend to the vendor community?

COTS vendors should strategically identify where their technology fits into each of the functional areas of CDM. They should promote their technologies with tailored messages that clearly and succinctly describe where they fit within this solution. The prime contractors are really working hard to understand a number of COTS products and how multiple technologies integrate into an interoperable and scalable solution, so they are not going to have a lot of time to teach themselves the key differentiators of each COTS product. It's absolutely crucial as a technology vendor that you clearly map your true capabilities to the functional areas to help the Primes understand the need for your solutions to improve positioning in response to CDM solicitations. Do not try to squeeze square pegs into round holes. The Primes are working with multiple vendors and you can quickly lose credibility with these strategic CDM partners if there is a perceived waste of time "pitching" a solution that might not be a best fit for a particular functional area. Vendors really should focus on honing their message to highlight their strengths and how those align to the proper functional areas.

What does it mean to be secure?

Enforcing a dynamic cybersecurity risk management policy is crucial to being secure. This policy needs to be thoroughly understood and adopted by all stakeholders, both internal and external—those accessing your data, your network, and your resources. This policy cannot be stagnant; it must adapt to evolving threats to the network. It should enable risk-based decision-making, aligned to your mission and business objectives. Your users will always be the weakest link in the chain, so it's essential that all levels of the workforce participate in continuous cybersecurity education in order to understand the risk they pose as users of the network, and how they can eliminate those risks.


GOVLOOP GUIDE
THE VIRTUAL PLATFORM
CITIZEN ENGAGEMENT
BLANKET PURCHASE

STRATEGIC SOURCING: THE DHS & GSA BLANKET PURCHASE AGREEMENT

To streamline the procurement process, the General Services Administration and DHS have collaborated to create an acquisition vehicle, a blanket purchase agreement (BPA), for continuous diagnostic solutions. The BPA providesa way for agencies to make the most of strategic sourcing to purchase CMaaS solutions. It's available to federal, state, local and tribal government entities, it provides a consistent and standardized method of identifying and mitigating the effect of emerging cyber threats, and it capitalizes on the strategic sourcing capabilities to minimize costs.

The benefits of the BPA have already been seen.

"When the first task order went out, we found that we were able to negotiate with the vendors that had won the CMaaS contract, an average of a 30 percent reduction on GSA's schedule prices and budget," Streufert said.

The CDM tools/CMaaS BPAs have been awarded in accordance with Federal Acquisition Regulation 8.405-3 and GSA IT Schedule 70 contracts. GSA estimates that there is a combined $6 billion ceiling over five years for this contract vehicle. The BPA offers three options for ordering CMaaS solutions:

- *Direct Order/Direct Bill: This option can be used to procure products and/or services from the CDM Tools/CMaaS BPAs via Delegated Procurement Authority (DPA). Additionally, state, local, regional and tribal governments can use it.*
- *Assisted Acquisition/Consulting: Federal agencies' can use assisted acquisition services from GSA's Federal Systems Integration and Management Center or a Customer Service Center of the Federal Acquisition Service's Regional Office of Assisted Acquisition Services to acquire full lifecycle acquisition support for their procurement of CMaaS products and services.*
- *Strategic Sourcing with DHS: This option leverages DHS' DHS process to procure products and/or services from the BPA.*

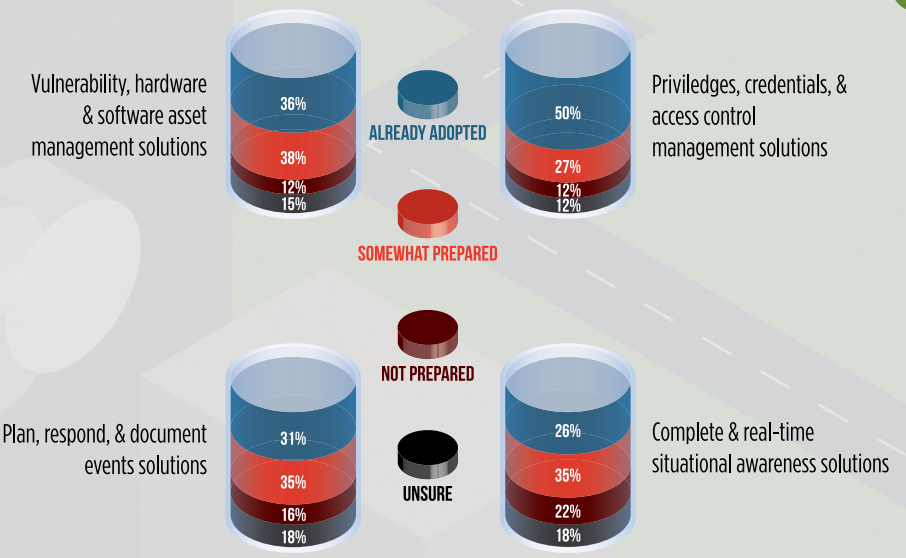
As noted, CDM is not just for the federal government. State, local and tribunal government entities are eligible to participate in the program. "The cooperative purchasing program of the General Services Administration, allows states and local governments to make purchases off of GSA schedules consistent with the laws and regulations that may exist at the state and local level," said Streufert.

The benefit for state and local governments, which can also use GSA schedules for CDM purchases, is that they can buy with quantity discounts that have been assembled at the federal level. Additionally, they can receive assistance to complex contracts, which have already been designed and set up for similar entities.

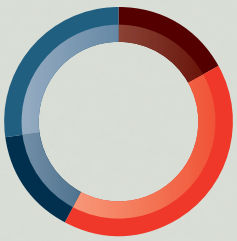
Streufert expects all civilian agencies to eventually participate. "Where participation is being delayed or they may not be as active, it is because they're just so small that the need for a full-blown security program is less," he said. "There've been a number of the departments and agencies in the civilian side of government that have asked to rather than avoid participation, delay [their] participation. That had to do with the fact that arrangements that were in place to manage their technology at the department or agency were about to change, and they were reluctant to get a program started when they expected to award a new contract and bring in a new team, and this was just to conserve resources."

Figure 4.

To find out agency's maturity levels and preparedness for CDM, we asked: How would you assess your preparedness level to adopt the following types of continuous monitoring solutions?



Where do you have the largest gaps in your cybersecurity solutions?



17% ENDPOINT INTEGRITY

41% LEAST PRIVILEDGE & INFRASTRUCTURE INTEGRITY

15% BOUNDARY PROTECTION & EVENT MANAGEMENT

27% ALL OF THE ABOVE

THE 3 PHASES OF CDM & 15 CONTINUOUS DIAGNOSTIC CAPABILITIES

CDM consists of 15 continuous diagnostic capabilities, covering three separate phases of deployment. Each phase has been defined by the GSA Ordering Guide, an essential read for anyone looking to become involved in the CDM program. Here are the guide's key sections and lessons. Our survey also explored agencies maturity level to adopt CMaaS solutions, which is important to understand as we explore the 15 continuous diagnostic capabilities. The full findings can be found in Figure 3.

CDM Phase 1: Foundational Elements to Protect Systems and Data

❶ *Hardware Asset Management: works to discover unauthorized or unmanaged hardware on government networks.*

❷ *Software Asset Management: works to discover unauthorized or unmanaged software on government networks.*

❸ *Configuration Management: finds misconfiguration of hardware devices (physical, virtual and operating systems) and software.*

❹ *Vulnerability Management: used to discover and support remediation of known IT vulnerabilities on a network.*

CDM Phase 2: Least Privilege and Infrastructure Integrity

❶ *Manage Network and Asset Controls: provides an agency the ability to remove and limit unauthorized network access, which will prevent hackers from gaining access to data at rest or in motion.*

❷ *Manage Trust in People Granted Access: prevents insider attacks by screening new and existing individuals who have access to the network.*

❸ *Manage Security-related Behavior: prevents general users from taking unnecessary risks and allowing hackers to successfully deploy social engineering attacks.*

❹ *Manage Credentials and Authentication: manages the credentials used to access networks, and proper management leads to reduced hijacking and unauthorized use of logins and passwords.*

❺ *Manage Account Access: limits unneeded accounts to reduce risk of access to unauthorized data.*

❻ *Prepare for Contingencies and Incidents: calls for prevention preparedness in the case of unanticipated events or attacks.*

CDM Phase 3: Boundary Protection and Event Management for Managing the Security Lifecycle

❶ *Respond to Contingencies and Incidents: supports preventions of repeat attacks, ends ongoing attacks and strategizes ways to stop attacks from known weaknesses.*

❷ *Design and Build in Requirements Policy and Planning: reduces the attack surface and identifies the areas of a system most vulnerable.*

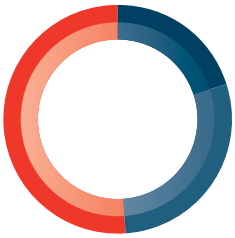
❸ *Design and Build in Quality: prevent attackers from exploiting weaknesses by finding the most vulnerable aspects, prioritizing risk and solving the worst problems first.*

❹ *Manage Audit Information: uses audit information to identify and respond accordingly to prevent persistent attacks.*

❺ *Manage Operation Security: prevents attackers from exploiting weakness by improving the way administrators authorize operation of systems.*

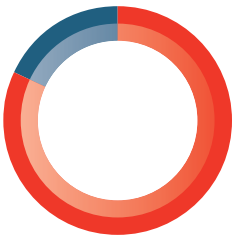
Figure 3.

Are you considering procurement of CDM-like technologies with your own funding?



20% INTEND TO
29% YES
51% NO

Is your agency participating in the CDM program?



82% NO (will partner with DHS)
18% YES

What are the challenges to adopt CDM?

20% SLOW PROCUREMENT PROCESS
10% UNDERSTANDING PROGRAM FUNDING
12% UNDERSTANDING PROGRAM BENEFITS
14% UNDERSTANDING CDM PROCUREMENT
13% ALREADY HAVE A SOLUTION
31% UNSURE OF A SOLUTION

The future of technology is more secure than ever.

Intel® Security combines the expertise of McAfee® with the performance and trust of Intel to deliver secure computing to consumers and businesses worldwide. We believe that as technology becomes more deeply integrated into life, security must be more deeply integrated into technology. Because when everyone has the confidence to use technology to its full potential they can achieve their full potential. Visit intelsecurity.com. McAfee is now part of Intel Security.

WHY NETWORK VISIBILITY IS ESSENTIAL TO YOUR CYBERSECURITY PROGRAM

Patrick Flynn, Director, Homeland/National Security Programs, Intel Security, shared his thoughts on CDM, and how Intel Security can help agencies participate in the program.

What kind of opportunities does CDM present for government?

While CDM allows agencies to deploy technology that will enhance the security and resilience of their networks, better safeguarding both the sensitive data on those networks and the critical functions they provide to all Americans, the primary benefit is the ability to get on the same sheet of music. CDM will create efficiencies, cost-savings and ultimately a higher level of cybersecurity. DHS has done a very positive thing getting this [program] out.

Why is visibility essential to the CDM program?

What visibility provides is the ability to manage those different types of managed points, and endpoints can be a classified in a lot a different ways. The end points could be computers or mobile devices, so agencies need to be able to take that inventory, understanding what's touching their network, and be able to move manage those assets in literally seconds, instead of hours. CDM will eventually bring that visibility to the consumer base.

How can Intel Security help agencies as they look to join the CDM program?

Our overall push and our message to agencies is that we're open, we're integrated, and we develop a common framework through our secure innovation alliance. Our security vision helps you increase the capabilities in a very dynamic world, a very evolving and threatening world. And again, over the lifecycle of your assets, we help agencies in a cost constrained environment reduce their overall budget signature.

How does open-source come into play?

Intel Security really wants to break down the barriers, and we want to break down the silos and generate solutions that are open. One of the preeminent things is the ability to share information and Intel Security really spends a lot a time in developing solutions that are totally open, that you can literally take anything and with a few tweaks you can integrate the benefits of that niche solution into the overall way of how it gets reported. Intel Security has spent a lot a time and is committed to this, and our customers have benefited greatly.

Intel Corporation recently acquired Intel Security; can you provide a status update?

It has been almost three years now since the Intel Corporation bought Intel Security. One of the things that a lot a people don't really appreciate yet is the fact that Intel, the infrastructure manufacturer, bought Intel Security, the chip manufacturer, so they can now design security into the silicon. Being able to turn things on at the silicon level is immensely more secure than adding in layers. It changes the dynamic worldwide. And it's happening now.

Patrick Flynn's comments remind us of the complexity of cybersecurity, and that by gaining improved visibility, agencies can improve how they protect critical infrastructure.

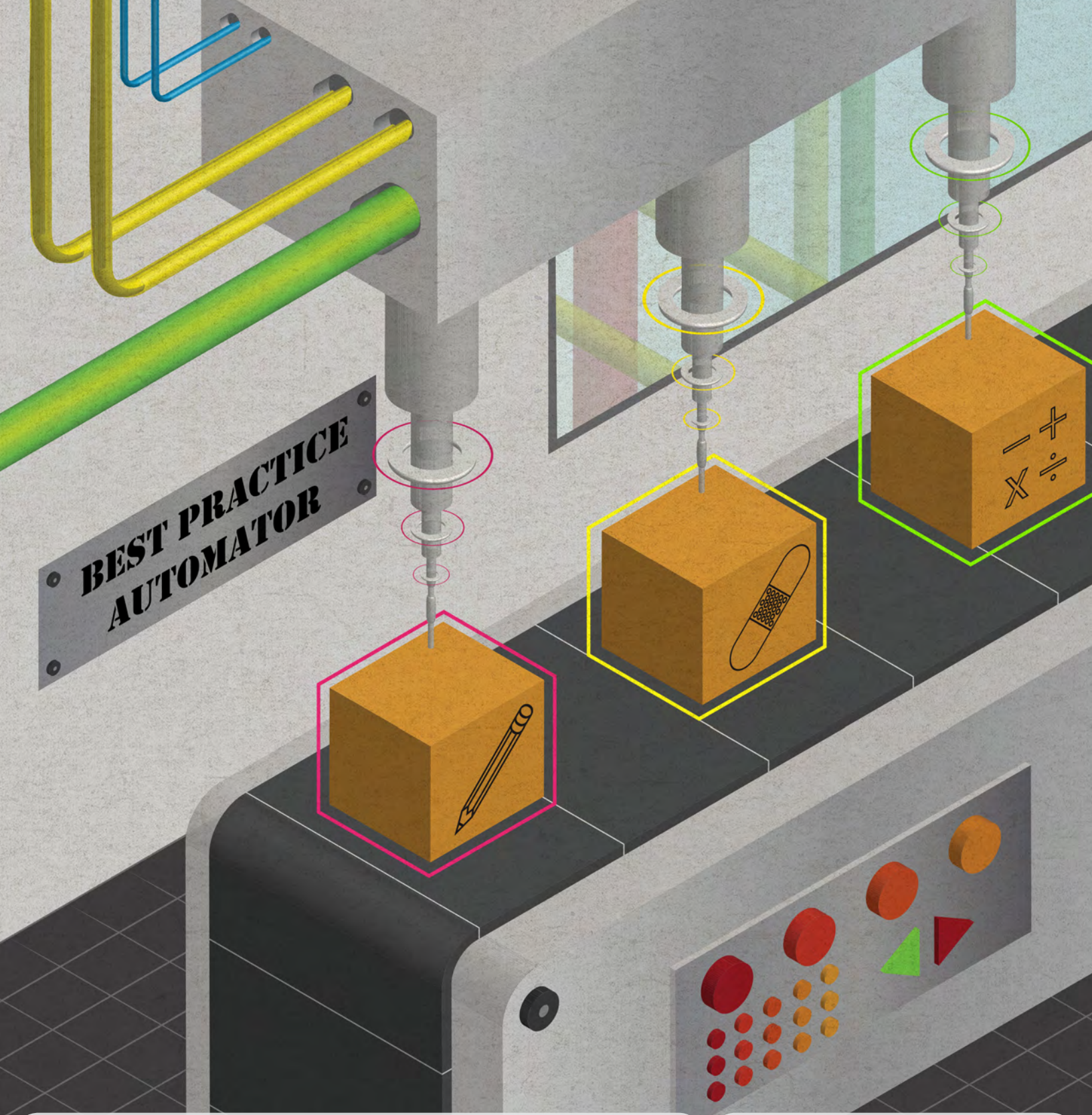
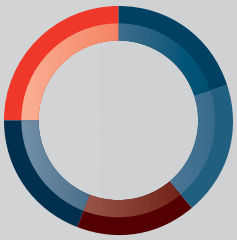


Figure 5.

What does our government audience believe are the benefits of the CDM program?



20% IMPLEMENT SENSORS & DASHBOARDS FOR REAL-TIME ANALYSIS

19% IDENTIFIES VULNERABILITIES IN MINUTES

17% MITIGATE FLAWS IN NETWORK SECURITY

19% DECREASES RISK OF ATTACKS

25% LEVERAGE THE COLLECTIVE BUYING POWER OF THE GOVERNMENT TO REDUCE TECHNOLOGY COSTS

Figure 6.

We asked the GovLoop community: What's more important to your organization, compliance or security?

37% COMPLIANCE

63% SECURITY

9 BEST PRACTICES FOR CDM SUCCESS

The CDM program has many benefits for agencies, according to responses to our survey. We explore all of them in Figure 5, but the leading response was CDM lets agenices "leverage the collective buying power of the government to reduce technology costs."

"The key elements of the program revolve around understanding the known security risks that exist on their networks and their software applications, their systems, with special attention to those that are listed with moderate risk and high risk," Streufert said.

Based on our survey and other research, we identify the nine best practices for CDM, and what you need to consider as you begin to participate in the program.

❶ Conduct Routine Testing.

By routinely testing networks to find known vulnerabilities, agencies can deal with the worst problems first. "The idea of doing the security testing more frequently as a best practice to queue up the list of previously known problems, and a dashboard displaying those results, and working on the worst problems first, are kind of at the top of the list of best practices that are being encouraged," Streufert said.

❷ Understand the National Vulnerability Database Guidelines to Rank Vulnerabilities.

The National Institute of Standards and Technology's National Vulnerability Database is a government repository of standards-based vulnerability data. It helps agencies automate security-related reporting, understand if they are FISMA-compliant and conduct vulnerability management and security measurements. By ranking your vulnerabilities, you will be able to gain essential information about your network. This will also help you tackle our next best practice, which is to solve the worst problems first.

❸ Solve Your Worst Problems First.

As you look at the NIST rankings of known security flaws, your agency should tackle the best known ones first and work down to less serious risks. This will help you remove the greatest percentage of problems on the network. Without CMaaS solutions, this process is very difficult for agencies to manage.

❹ Establish a Common Measure of Risk for Like Problems.

"Another example of a best practice is to establish a common measure of risk for like problems across the organization, so that there can be what we call an apples-to-apples comparison of risk in one organization vs. another inside of the Cabinet, department or agency," Streufert said. "That allows the managers to judge how their progress compares to their peers."

❺ Automate as Much of the Security Testing as Possible.

Agencies should look to automate as much of the security testing as possible and move away from manual testing. With automation, the frequency and comprehensiveness of coverage can improve. Through automation, there has been steady progress at several departments and agencies toward reducing risk by as much as two-thirds or as much as a factor of 10, which is what State achieved in 2009, Streufert said.

"For every action you take on security, you're not only able to make the dollar go farther, but the cost per transaction and repair action is going down through the benefits of automation," Streufert said.

❻ Leverage the Power of Strategic Sourcing.

Strategic sourcing is an analytical process that is used to reduce total cost of ownership (TCO) and improve service delivery for agencies. GSA provides a list of benefits for strategic sourcing that includes:

- *Lower spending levels*
- *Lower TCO*
- *Clearly defined requirements*
- *Acquisition aligned with mission requirements*
- *Managed vendor performance*
- *Increased achievement of socioeconomic acquisition goals*
- *Increased achievement of "green" goals*
- *Improved vendor access to business opportunities*

With DHS and GSA working together to provide a strategic sourcing opportunity through the BPA, agencies have a unique chance to adopt CMaaS solutions. "We have memorandums of agreement with 108 of 124 dot-gov organizations for CMaaS," Streufert said. "This allows the departments and agencies of civilian government to combine their purchasing power for the best reductions in cost."

❼ Use CDM to Achieve Improved Compliance and Security.

Compliance and security do not have to be at odds with each other. In fact, often they're complementary. (See Figure 6.)

"The way that we look at security automation is simply providing a set of tools to those that are upholding that original mandate to be both cost-effective and risk-based," Streufert said. "We're simply able to cover more ground in less time at lower cost than was previously possible. We find that after automation of security testing is active and that good dashboards are in place, that actually those that are looking after the processes and those that are concerned about operations have a common reference point which is mutually beneficial to both of them."

❽ Make Collaboration a Priority.

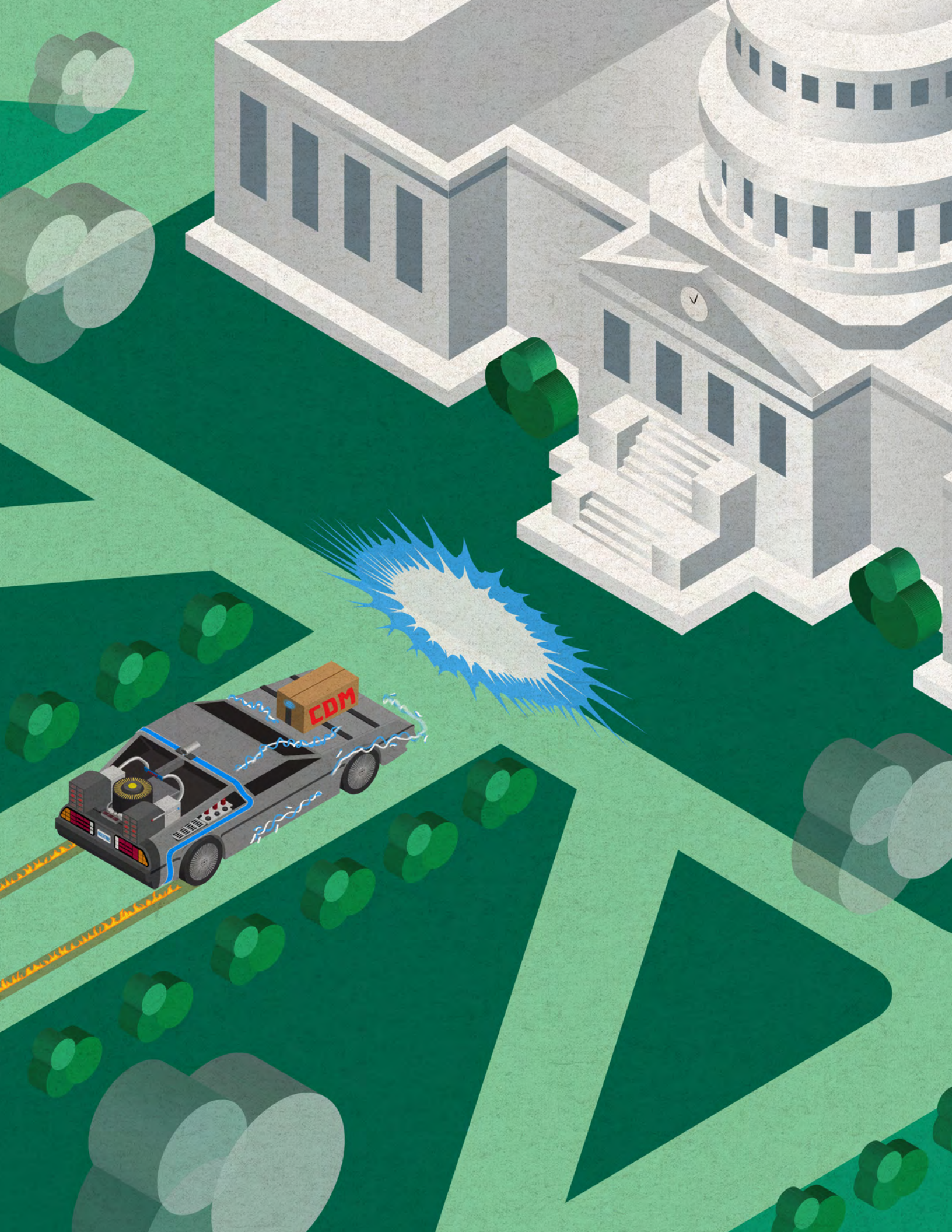
Collaboration is an essential part of any cybersecurity program. Organizations must be able to share information on compliance and reporting. Also, leaders must work closely to engage frontline staff to make sure that technology will help improve their jobs and ease the burden of manual processes.

"We can't forget to mention the business managers of the department and agency, whether at the working level or the executive level," Streufert said. "If the security policy and compliance people and the operational people are working well together, then business operations can proceed with fewer interruptions, allowing really every member of the department or agency to be ahead as a result of the collaboration."

❾ Embrace Cybersecurity at the Highest Levels.

In order to fully adopt CDM and change the mind-set of cyber professionals, government agencies must have top-down leadership on cyber projects. Cybersecurity is the shared responsibility of an entire agency and requires a commitment to excellence and a cultural approach around security.

These best practices are just the start of improving security at your agency. To fully capitalize on CDM, agency leaders must commit to understanding cybersecurity and learn how technology can improve service delivery and maintain the much-needed security requirements to stay secure in a constantly evolving threat landscape.


CDM

THE FUTURE OF CDM

CDM is bound to have a long-reaching impact on the security efforts of our country. But new threats will continue to emerge and risks will increase even as new technology solutions are deployed.

The next steps for the program are to continue moving through its three planned phases and incorporate workforce training along the way.

"There are some efforts under way to strengthen training for the users that are at the federal government level, and we're publishing some online training that can be accessed from our website, and would also be available for use by the state and local governments that may want to take advantage of it," Streufert said.

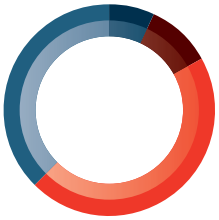
Additionally, the goal of CDM is to be sure that all agency networks can conduct basic diagnostic testing capabilities. "The future is to round out the current capabilities to be comprehensive and provide diagnostic testing against the risks that are most prevalent. We expect to be at this for a period of additional years until basic capabilities cover all networks and the custom applications," he said.

In the long run, the program will be expanded from basic diagnostic and mitigation capabilities to protecting custom software that government agencies are creating. Streufert notes that these plans are slated for 2016 and tentatively defined as "critical application resilience."

"We are also making our contract of diagnostic tools available to cloud providers that will help them in cost-effective ways to meet the security needs of those departments and agencies and application managers that want to operate out of cloud environments," Streufert said.

"In a small way, we hope that as this program goes forward, that we're going to have a tool that will ultimately benefit everyone in the organization as well as taxpayers and businesses that interact with the government," he said "They'll sleep better at night knowing that their information is safer."

Figure 7.



7% CDM WILL HAMPER MY ABILITY TO DECIDE WHAT WILL BE IMPLEMENTED ON MY NETWORK TO SECURELY ACCOMPLISH MY MISSION

10% NO IMPROVEMENT

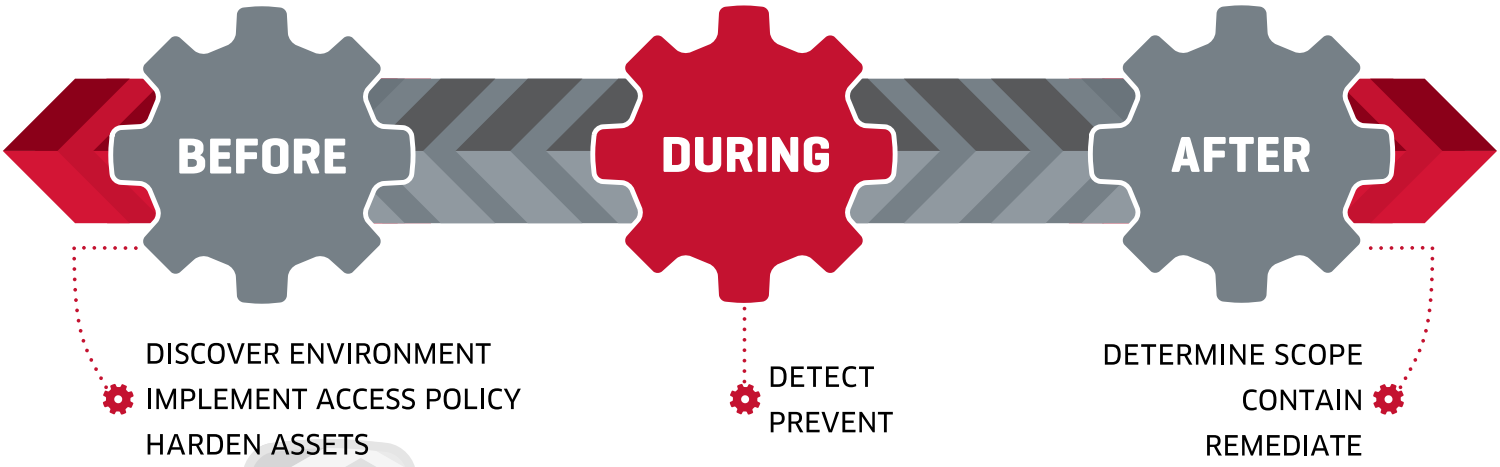
45% MOVING IN THE RIGHT DIRECTION, BUT WE'RE STILL NOT WHERE WE NEED TO BE

37% THIS WILL STRENGTHEN OUR NETWORKS TO HELP US MORE SECURELY ACCOMPLISH OUR MISSION

The New Security Model

BEFORE, DURING AND AFTER™ AN ATTACK

The New Security Model means
accounting for the entire attack continuum



A CONTINUOUS SECURITY PROCESS TO RESPOND TO CONTINUOUS CHANGE

ADVANCED MALWARE PROTECTION: A NECESSITY IN YOUR CYBER ARSENAL

Steve Caimi, Industry Solutions Specialist for Sourcefire (now part of Cisco), spoke with us about the opportunity which CDM presents, and how Sourcefire can help agencies prepare.

What kind of opportunities does CDM present for government?

CDM presents great opportunities for agencies to strengthen security postures and become more effective. DHS has done a great job of stating their goals for the program. It's about adopting a threat-centric approach to security to combat threats to the nation's networks in real time. The opportunities fit into four areas:

❶ **Gaining Visibility:** Examining the first phase of CDM for example, it covers hardware/software asset management and endpoint integrity, which speaks to knowing what's out there. Do agencies know what systems and devices they've deployed? With the right sensors, dashboards, and real-time information they'll have the ability to see everything with the right context to make informed decisions and take immediate action. So with the right capabilities, gaining visibility into what's out there, you'll know about the applications running and operating systems present.

❷ **Being Threat-focused:** Today's attacks are happening at lightning speed, and threats can originate from the outside or the inside. With the right threat-focused capabilities backed by the best security intelligence you can identify the biggest threats and address them first. Decisions must be analyzed continually – not just at a point in time – so that the most current information can be used in the decision-making process. So with a threat-centric approach to security, you can address the entire attack continuum – before, during and after an attack. CDM does two things – forces agencies to remember not to take their eyes off the ball – stopping the threat is job one – and motivates federal agencies to revisit technologies to ensure they have the best solutions present to detect, understand and stop threats, pursuant to true spirit of CDM.

❸ **Consistent Control:** Once you know what's out there and have technologies with advanced threat detection, then it's about consistent control. Once a threat is detected, you want automated enforcement to stop the threat across extended networks simultaneously. Consistent policies across the network and data center lower operational risk by identifying and resolving problems faster than ever.

❹ **Complexity reduction:** Today's government networks are fragmented and complex. The right CDM solutions adapt to changing dynamics -- at scale and securely -- to reduce complexity and improve security through unified management, automation, APIs, and so forth. CDM solutions that are platform-based and cover network to devices out to the cloud make for extensible technology with unified policy and consistent controls versus mere point security appliances.

Can you speak more about Cisco Advanced Malware Protection (AMP)?

In today's environment, malicious code is created and QA tested against leading "point-in-time" anti-virus software before being released, which ensures malware infections. Malware today evades point-in-time detection methods because it's designed too.

Cisco AMP , however, delivers continuous monitoring through a powerful combination of point-in-time and continuous, retrospective security capabilities.

We do a lot of heavy lifting in our security intelligence cloud to deliver continuous capability.

This means determining a file's malware disposition at an initial point-in-time and also continuously tracking and analyzing the file – always watching its activities. This amounts to a 'continuous' capability that persists after the file has moved across the network or endpoints. A file thought to be good/unknown initially but is later identified as malicious can be retrospectively identified to remediate malware and contain outbreaks.

Caimi's insights are evidence that as the CDM program becomes more widely adopted, governments overall ability to secure systems will increase.

YOUR CONTINUOUS DIAGNOSTIC & MITIGATION CHEAT SHEET

LOOKING TO GET SMART ON THE CDM PROGRAM? LOOK NO FURTHER.

THE CDM ELEVATOR PITCH & TALKING POINTS

As our systems have become more interconnected and diverse, the risk of cyberattack has increased. The Homeland Security Department has come up with a great way to standardize the assessment and mitigation of risks in a way that can also be shared governmentwide. It's called the Continuous Diagnostic and Mitigation Program. It works through sensors that scan for known cyber flaws and dashboards that collect the results and compile them into customized reports.

the 3 phases of CDM

1. ENDPOINT INTEGRITY
2. LEAST PRIVILEGE & INFRASTRUCTURE INTEGRITY
3. BOUNDARY PROTECTION & EVENT MANAGEMENT

CDM MUST READS

- "OMB Directive 10-15: FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management"
- "OMB Directive 10-28: Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security"
- "NIST 800-30: Guide for Conducting Risk Assessments"
- "NIST 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach"
- "NIST 800-39: Managing Information Security Risk"
- "NIST 800-53 Rev. 4: Security and Privacy Controls for Federal Information Systems and Organizations"
- "NIST 800-137: Information Security Continuous Monitoring for Federal Information Systems and Organizations"
- GSA Ordering Guide for CDM and CMaaS solutions

(Click to follow links)

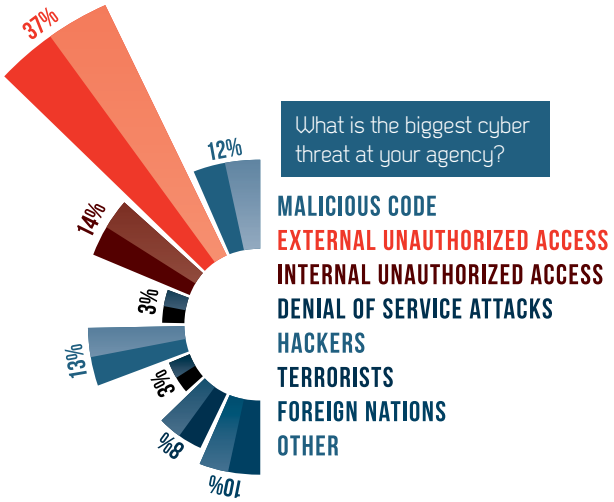
TOP 10 BENEFITS OF CDM

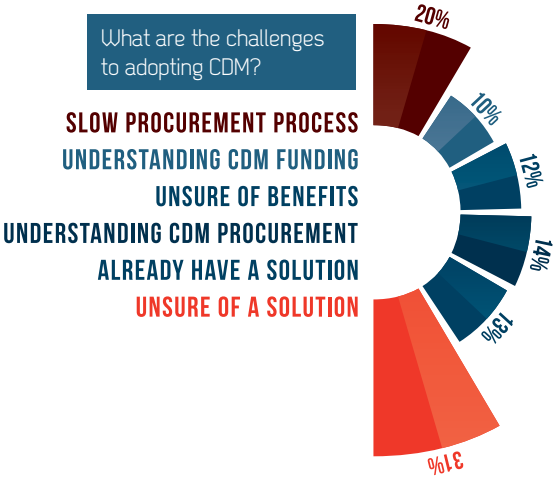
To support the move to provide risk-based protections and broader visibility to agencies, CDM helps agencies procure a suite of tools that will:

1. Provide cyber professionals with real-time analysis of their network.
2. Assess risks and threats.
3. Mitigate and identify flaws at near-network speed.
4. Create a smaller attack surface and decrease risk for dot-gov networks.
5. Find weaknesses and vulnerabilities.
6. Improve hardware-asset management for dot-gov networks.
7. Improve software-asset management for dot-gov networks.
8. Improve vulnerability management for dot-gov networks.
9. Create CDM dashboards to show network security.
10. Improve the management and trust of people granted access on a network.

THE 15 CONTROLS OF CDM

1. Hardware Asset Management
2. Software Asset Management
3. Configuration Management
4. Vulnerability Management
5. Manage Network and Asset Controls
6. Manage Trust in People Granted Access
7. Manage Security Related Behavior
8. Manage Credentials and Authentication
9. Manage Account Access
10. Prepare for Contingencies and Incidents
11. Respond to Contingencies and Incidents
12. Design and Build in Requirements Policy and Planning
13. Design and Build in Quality
14. Manage Audit Information
15. Manage Operation Security





9 BEST CDM PRACTICES

1. Do routine testing.
2. Follow NIST guidelines to rank vulnerabilities.
3. Solve the worst problems first.
4. Establish a common measure of risk for like problems.
5. Automate as much of the security testing as possible.
6. Explore strategic sourcing.
7. Use CDM to achieve improved compliance and security.
8. Focus on collaboration.
9. Embrace cybersecurity at the highest levels.

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 140,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to Patrick Fiorenza, senior research analyst, GovLoop, at pat@govloop.com.

GovLoop
1101 15th St NW, Suite 900
Washington, DC 20005

Phone: (202) 407-7421 Fax: (202) 407-7501

www.govloop.com
Twitter: @GovLoop

ACKNOWLEDGEMENTS

Thank you to immixGroup and their partners HP, FireMon, Intel Security, and Sourcefire for their support of this valuable resource for public-sector professionals.

Author: Patrick Fiorenza, GovLoop's senior research analyst

Designers: Jeff Ribeira, GovLoop's senior interactive designer, and Tommy Bowen, GovLoop's junior designer.

Editor: Catherine Andrews, GovLoop's director of content

GOVLOOP FIELD NOTES

1101 15TH ST NW, SUITE 900
WASHINGTON, DC 20005
PHONE: (202) 407-7421
FAX: (202) 407-7501