

FACE OF FACE CYBER SECURITY

SPONSORED BY:



CDM and Cybersecurity Evolve With the Times



Simplee/Shutterstock.com

As the CDM program evolves, agencies must change processes as well as technology

EVENT OVERVIEW

The variety and volume of cyberthreats continues to increase, especially as cloud computing, the Internet of Things, and mobile computing continue to increase in popularity. Securing government agency networks is a complicated and constantly evolving task, requiring the right mix of technology tools, business savvy and workforce

expertise. Agencies have to manage evolving network dynamic, according to industry and government speakers at a recent event.

One way the federal government hopes to help agencies better defend against the constantly evolving nature of cyberthreats is the Continuous Diagnostics and Mitigation (CDM) program. CDM provides tools and services to help agencies identify and respond to this evolving risk, whether it's pro-

tecting device or software assets, user credentials, data or ultimately the network boundary.

So far, CDM has made progress in several areas. It has helped agencies develop a better understanding of their assets, increased standardization of security tools, deployed numerous sensors, and developed agency dashboards, among other successes, says Kevin Cox, CDM Program Management Office Program Manager, DHS.

For more information on Face to Face Events go to: www.1105publicsector.com/events

The CDM program quickly removes the easy targets, such as unpatched systems that make it easy for adversaries to access and compromise data, he says. There is still work to be done to complete the first two phases of the program, which focus on managing the “what” and the “who” on the network. By the end of 2018, CDM will be able to identify what systems are well patched and well configured, and get resources to fix any problems.

“In many ways the technology is the easy part. It’s the process reengineering, it’s the training, it’s the governance that often times is difficult,” says Cox.

Focus on the People and Process

Phishing is one example of a security problem agencies can address with proper training. Even agencies with strong firewalls, and intrusion prevention and detection can still be felled by a phishing scam that opens the door for an attacker to introduce malware onto the network.

How can an agency take control of the situation? By building a comprehensive security program that addresses not only the technology, but also people and process, says Stephen Nardone, Director of

Security and Mobility Practices, Connection Public Sector Solutions.

“The technology does exist, but it’s how the users are using the technology and are they actually behaving in safe and secure ways, [that] is really the key,” he says.

Network attacks are increasing because the methods are improving, and it’s cheaper and easier to launch one. Traditional DDoS attacks are launched from computers. With the proliferation of cloud infrastructures people are able to launch large-scale attacks at minimal cost, says Jerry Petrosino, CISSP, Senior Solutions Engineer, Akamai Technologies.

“We are beginning to see a very large increase in volumetric attack and also the packet per second that those devices can handle,” says Petrosino. Hacking, he says, has become a service with no expertise needed.

That is one of the reasons network visibility is essential. As networks grow they typically evolve; becoming larger, more complicated, and more difficult to secure, says Tom Kopko, Senior Director, Gigamon.

The goal is pervasive visibility across all environments, whether physical, virtual or in the cloud. This means getting network traffic to the tools so they are

able to do their job. “If a tool can’t see a particular packet it certainly can’t secure it,” says Kopko.

One approach is to use the network as a sensor to identify suspicious traffic and act on it; and as an enforcer to enforce policy and enforce access policy, and drive segmentation, in a scalable and manageable way. It’s hard for agencies to know if someone is using an unauthorized device, or whether certain user behavior is risky, says Steve Caimi, Industry Solutions Specialist, Cisco.

Network equipment can provide “insight into what systems are talking to what, [and] trace the information back to what users are doing and when they are doing it,” he says.

CDM Acquisition Changes

When it comes to cybersecurity, agencies must remain flexible. That extends to the CDM acquisition process as well. The CDM blanket purchase agreement (BPA) expires in August of next year. The General Services Administration (GSA) is taking the opportunity to create something better.

GSA plans to replace the BPA with a special item number (SIN) CDM product catalog of tools under IT Schedule 70. This is intended to make it easier for agencies to buy extra licenses or emerging tools,

“In many ways the technology is the easy part. **It’s the process reengineering, it’s the training, it’s the governance** that often times is difficult.”

—KEVIN COX, CDM PROGRAM MANAGEMENT OFFICE PROGRAM MANAGER, DHS

A man in a white shirt and dark pants stands on a rooftop, looking out over a dense city skyline at sunset. The sky is filled with dramatic, colorful clouds. Large, white, sans-serif text is overlaid on the image, reading "THERE'S NEVER BEEN A BETTER TIME".

THERE'S NEVER BEEN A BETTER TIME

to worry less and innovate more

"Are we secure? Are we innovating?" Good questions. At Cisco we know that the more effective and simple your security solutions are, the more you can push the boundaries of what is possible. See why there's never been a better time to use security to spark your next great idea at cisco.com/neverbetter

EVENT OVERVIEW

better support the CDM lifecycle, and make it easier for new vendors to join, says Jim Piche, Homeland Sector Director, FEDSIM, GSA.

The SIN would have a high ceiling and broad scope incrementally funded by DHS or distributed through the agencies, says Piche. “We want to break the cycle of continuous acquisitions,” he says. “This is the continuous diagnostics program, not the continuous acquisitions program.”

CDM is a part of a portfolio of shared services in government that has helped agencies work together, save money, better manage systems, increase standards, and create awareness of what systems they have, says Mark Kneidinger, Director, Federal Network Resilience, U.S. Department of Homeland Security.

“CDM is not only a good example of a shared service, but also a replicable model as we take a look at other new programs coming forward,” he says. DHS plans to work closely with GSA to see how cybersecurity shared services could evolve in the future.

What makes CDM a shared service? It brings together industry leading practices and technology; helps consolidate processes, systems and workforces; delivers services across complex federated

customers; is customer focused; and demonstrates efficient aggregation of resources.

“Think about shared services as an opportunity to get away from having to build each and every service that we have from soup to nuts, on our own, and by ourselves,” says Robert Wuhrman, PMP, CISSP, Enterprise Architect, Unified Shared Services Management, GSA. USSM is establishing a framework to help lines of business develop the government-wide requirements that can lead to shared knowledge, and acquisition efficiencies as solutions are put in place.

The CDM program has helped the Department of Commerce realize an enterprise approach can be successful, says Rod Turk, Deputy Chief Information Officer and Chief Information Security Officer, Department of Commerce. “We’re all in when it comes to the CDM program,” he says. “It has allowed us to change some attitudes, to create a little bit of a different culture and move toward that change model.”

CDM focuses on three areas: change, capabilities and culture, he says. Agencies should not be afraid of change, such as centralizing procurement. They should take advantage of the capabilities that CDM offers, such as asset and software management. Ultimately,

agencies need to develop a culture that incorporates cybersecurity into the system development lifecycle, planning for it at the beginning and making it part of the cost model.

In an era of shrinking budgets, funding security is an issue for agencies, but CDM relieves some of this pressure as well. “[CDM not only provides] a baseline for your continuous monitoring strategy... [but] the best thing is that the bulk of it is being paid for,” says Dwayne King, CISSP, PMP, Senior IT Specialist, OPM Cybersecurity Program, U.S. Office of Personnel Management.

The key highlights of CDM are reducing security gaps, vulnerabilities and risks, says King. OPM has been able to automate certain security features under the program that has helped it gain greater visibility of its assets and devices, patch security gaps, and enforce virtual private networks, among other improvements.

Effective security should be simple, open and automated, says Peter Romness, Cybersecurity Programs Lead, U.S. Public Sector, Cisco. “When we talk about pushing the boundaries of cybersecurity,” he says, “it’s how do we make sure that the technology that we have is properly utilized, so that it can serve its purpose which is to protect our national assets.”



“When we talk about pushing the boundaries of cybersecurity, it’s how do we make sure that the technology that we have is properly utilized.”

—PETER ROMNESS, CYBERSECURITY PROGRAMS LEAD, U.S. PUBLIC SECTOR, CISCO

Session Highlights

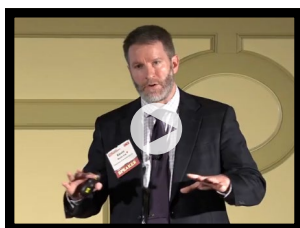
Here are some take-aways from the individual sessions

SESSION 1

CDM- Pushing the Boundaries of Cybersecurity

Speaker

Kevin Cox, CDM Program Management Office Program Manager, DHS



Kevin Cox

“In many ways the technology is the easy part. It’s the process reengineering, it’s the training, it’s the governance that often times is difficult.”

- The CDM program removes the easy targets, such as unpatched systems, that makes it easy for adversaries to access and compromise data.
- Currently CDM is focusing on phase 1 (what is on the network, creating a master device record) and phase 2 (who is on the network, creating a master user record).
- By the end of 2018, CDM will be able to identify what systems are well patched and well configured, and get resources to fix the problems.

Program successes include:

- Stronger understanding of assets in agencies
- Increased standardization of security tools

CDeploying agency dashboards

- \$600 million saved on products so far
- Shared services platform ready in Q3 FY17 for non-CFO Act agencies

By the end of the fiscal year, CDM will have deployed the majority of sensors in

phase 1 and rolled out agency and federal dashboards; gained visibility of general user credentials and privileged user access in phase 2; updated phase 1 to fill gaps in mobile and cloud computing; mature dashboards.

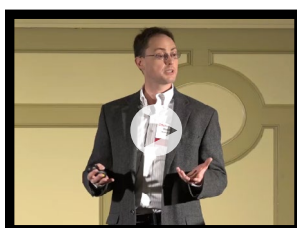
Phase 3 (what is happening on the network) will be tied to the next contracting approach. RFQs for this will be posted by this summer, with an award in the fall.

SESSION 2

Technology Insights I

Speaker

Steve Caimi, Industry Solutions Specialist, Cisco



Steve Caimi

“We can use the network itself as a sensor. The network equipment can give us that insight into what system are talking to what, [and] trace the information back to what users are doing and when they are doing it.”

- Effective cybersecurity risk management is the end goal for the CDM program.
- Hardware asset management—a focus on CDM phase 1—is especially difficult with mobile devices, but these assets must be profiled to see what is authorized and what is not.
- Cisco Identity Services Engine automates the process of discovering and identifying what devices are connected to the network, and removes them if they are unmanaged or unauthorized.

▪ Managing security related behavior is important in CDM phase 2; including seeing what people are doing on the network, whether they are taking unnecessary risks, and how that behavior affects the systems.

- The network can be used as a sensor to identify suspicious traffic and spot it for action.
- It’s difficult for agencies to manage boundary protection and network access controls when boundaries are broken down.
- Use the network itself to enforce network access policies, manage boundary protection, drive effective segmentation and build it into the network itself.

Speaker

Peter Romness, Cybersecurity Programs Lead, U.S. Public Sector, Cisco



Peter Romness

“It’s not just throwing technology at the problem; it’s providing the expertise, and the policy and the management that goes along with it.”

- The technology is the easy part—the people, policy and process are more challenging.
- Networks are hard to protect, mainly because of limited budget and lack of trained people.
- Many agencies are overwhelmed by number of security tools they have. Threats are more prevalent, networks are dispersed over the world, and people are overextended trying to defend the network.
- Agencies must make decisions about

COMPLIANCE

FedRamp / PCI / 508 / DNSSec / Rightsize CSP

SECURITY MITIGATION

Largest DDoS Attacks / Scalable DNS / BOT Mgmt /
Application Protection (XSS, SQL, LFI etc) / Network / Datacenter



Security Check

Akamai's highly distributed platform delivers applications consistently while providing control and security for Government users - **wherever they are.**

Session Highlights Continued

what is wrong and what requires attention, determine what risk level is acceptable, and take action as effectively and efficiently as possible.

- Cisco supports simple (to deploy, set up, grow and manage) open standards so products can work together, and automated functions for low level tasks and effective security.

SESSION 3

Acquisition Strategies: What's New in CDM Phase 3

Speaker

Jim Piche, Homeland Sector Director, FEDSIM, GSA



Jim Piche

“We want to break the cycle of continuous acquisitions. This is the continuous diagnostics program, not the continuous acquisitions program.”

- CDM acquisition successes include: more than 100 delegations of procurement authorities; a robust learning community with access to webinars, and learning programs; more than 169,000 approved tools in the catalog; saved average 30 percent on delivery orders, and 35 percent on task orders.
- There have been some CDM challenges. The BPA is expiring in August 2018, state and local access to CDM catalog has been challenging, current BPA limits contract type, it is not flexible enough to procure emerging products, it is difficult to increase the ceiling, and there is no option for flexible funding.
- GSA plans to create a special item number (SIN) to capture the CDM

product catalog of tools to replace the BPA, which expires in August next year.

- The RFI for the CDM SIN is out now with awards beginning in May.
- GSA plans to have a CDM SIN subcategory for emerging technologies/tools, make it easier for new vendors to join CDM program, have one SIN for CDM tools, and allow all buyers to purchase directly from seller/reseller.
- Draft acquisition milestones to look for: RFI for Phase 3 released in December 2016; RFI for Alliant Small Business released on March 6; industry day April/May 2017; Phase 1 TO2 series groups will be retained.

SESSION 4

Technology Insights II

Speaker

Tom Kopko, Senior Director, Gigamon



Tom Kopko

“Visibility is simply getting network traffic to tools so they can do their job. If a tool can’t see a particular packet, it certainly can’t secure it.”

- Pervasive visibility for CDM is required, however this is challenging because network infrastructures are chaotic, inefficient, without perimeters and difficult to secure.
- 75 percent of SecOps teams need better network visibility or have limited network visibility today; 85 percent of these teams say the complexity of network security operations is the same or more difficult than what it was two years ago.
- The Gigamon visibility platform helps agencies manage, secure, and under-

stand what is happening on the network so cybersecurity tools can do their jobs.

- The platform includes physical or virtual nodes, traffic filtering, and GigaSMART functions, such as de-duplication of packets, load balancing, and packet slicing.
- Gigamon also offers the ability to decrypt SSL traffic, load balance it across tools that are analyzing and securing SSL traffic, re-encrypt it and send it to its destination.
- Gigamon provides visibility into public cloud traffic, Internet of Things traffic, and has a rich set of APIs that allow for interaction and automated response among all the platforms.

SESSION 5

CDM and the Shared Services Approach

Speaker

Mark Kneidinger, Director, Federal Network Resilience, U.S. Department of Homeland Security



Mark Kneidinger

“CDM is not only a good example of a shared service, but also a replicable model as we take a look at other new programs coming forward.”

- CDM has already had an impact on agencies; helping them work together, save money, better manage systems, increase standards, and create awareness of what systems they have.
- CDM is a part of a portfolio of shared services, and a model of shared services that can be replicated in the future.
- CDM is a shared service because it brings together industry leading practices and

Protect Your Agency from Growing Threats

How Secure Is Your Infrastructure?



PROTECT. DETECT. REACT.

Breaches in the government/military sector
increased from 19% to 37% of total
breaches reported from 2015 to 2016.

Frequent and increasingly complex cyber attacks on U.S. business and government organizations are on the rise. It's clear that security is the most critical piece of the IT infrastructure, especially for the federal government. The team of experts at Connection® Public Sector Solutions has the knowledge and tools to assess the current state of your environment and build a unique solution to safeguard your infrastructure and data. We offer:

- Services designed to mitigate risk for your organization
- A cohesive, independent approach to information security
- Industry-leading assessments, analysis, technology planning, and integration



we solve IT™

Contact an Account Manager today to learn more.

1.800.800.0019 ■ www.connection.com/ps

Session Highlights Continued

technology; helps consolidate processes, systems and workforces; delivers services across complex federated customers; is customer focused; and demonstrates efficient aggregation of resources.

- DHS will work closely with GSA to see where the concept of cybersecurity shared services could evolve in the future.

Speaker

Robert Wuhrman, PMP, CISSP, Enterprise Architect, Unified Shared Services Management, GSA



Robert Wuhrman

“Think about shared services as an opportunity to get away from having to build each and every service that we have from soup to nuts, on our own, and by ourselves.”

- Shared services are those built with technology, tools, and services that are common and sharable among all agencies.
- Benefits of shared services include getting the government to a common standard for a given function or activity, such as continuous diagnosis and monitoring, gaining government-wide views and shared knowledge, and acquisition efficiencies.
- The function of Unified Shared Services Management office at GSA is to work across government and lines of business, such as cybersecurity, and look for opportunities to build shared services.
- There are managing partners for different lines of business who take a look at best practices and sit between the policy makers and the customers and providers.
- USSM is putting in place a framework to help the lines of business develop the government-wide requirements that can lead to shared knowledge and acquisition efficiencies as solutions are put in place.

SESSION 6

Technology Insights III

Speaker

Jerry Petrosino, CISSP, Senior Solutions Engineer, Akamai Technologies



Jerry Petrosino

“DDoS attacks are very problematic and very difficult for security teams to deal with, but most attackers use those as distraction devices to keep your guys occupied so they can launch more sophisticated attacks.”

- Akamai publishes threat data on a quarterly basis gleaned from more than 220,000 servers, deployed in more than 3,500 locations and 1,600 networks in 128 countries.
- Some types of attacks include Internet of Things attacks, such as the Miria Botnet that was used as a proxy attacker in Web application attacks and made sites unreachable.
- Largest attack on the Internet was a 620Gbps attack in September 2016.
- Traditional DDoS attacks are done from computers, but today with cloud infrastructure people can launch large-scale attacks at minimal cost.
- The United States is now at the top of the list of source countries for DDoS attacks mainly due to the Internet of Things botnets. It is also the first source of web application attacks.
- In the last quarter of 2016, three industries were targeted by DDoS attacks greater than 100 Gbps: gaming, media and entertainment, and software and technology.

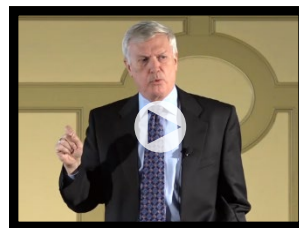
- In 2017, expect to see larger DDoS attacks, as well as an increase of Internet of Things attacks, credential abuse, hacking as a service and ransomware, and mobile device breaches.

SESSION 7

An Agency Perspective: U.S. Department of Commerce

Speaker

Rod Turk, Deputy Chief Information Officer and Chief Information Security Officer, Department of Commerce



Rod Turk

“We’re all in when it comes to the CDM program. It has allowed us to change some attitudes, to create a little bit of a different culture and move toward that change model.”

- There are three areas the government is focused on with CDM: change, capabilities and culture.
- Government agencies should not be afraid of making changes, such as centralizing procurement.
- Planning is important. Commerce had clients installed, some contracts in place, and training completed before CDM existed so it was able to jumpstart the program.
- The CDM program changed some mindsets—this can be done in an enterprise fashion and can be centralized within a Commerce component.
- Commerce is doing a phase 1 pilot and considering phase 2.
- Commerce wants to develop a culture of cybersecurity. This includes

Session Highlights Continued

involving cybersecurity in the system development lifecycle, planning for it at the beginning, and making it part of the cost model.

- The dashboard in the CDM program also creates a culture change because it will be readily available, easily updated, and allows report to be shared on a broad level.

SESSION 8

Technology Insights IV

Speaker

Stephen Nardone, Director of Security and Mobility Practices, Connection Public Sector Solutions



Stephen Nardone

“Even though you may not consider yourself an interesting target, you could be a good learning target for any cybercriminal out there.”

- The first step in talking about information security, is talking about business processes.
- Any time you have disruption, you have an increased risk. Security threats are the biggest disruption to the workplace.
- Today’s business challenges include increasing cyberattacks and security breaches, well-funded and trained cybercriminals, and attackers who go unnoticed in agency networks.
- About 35 percent of IT leaders worry about malware tailored to specific audiences; and 42 percent see breaches due to employee error or negligence as a top issue.
- There were more than 34 million identity breaches against government systems in 2015. In 2016, that dropped to 13 million. The attacks decreased in the amount of information that was compromised, but the number of attacks increased.
- Phishing is a major concern in government.
- Agencies must have a comprehensive security program. Protect, detect and react are the three pillars of security management. It involves people, process and technology.
- Addressing sophisticated threats requires comprehensive security testing, sound backup and restore strategy, unified security stack, sandboxing, and virtualization.

SESSION 9

An Agency Perspective: U.S. Office of Personnel Management

Speaker

Dwayne King, CISSP, PMP, Senior IT Specialist, OPM Cybersecurity Program, US Office of Personnel Management



Dwayne King

“The cool thing about CDM is that it provides a baseline for your continuous monitoring strategy... the best thing is that the bulk of it is being paid for.”

- The key highlights of the CDM project are the reduction in security gaps, vulnerabilities and risks.
- Through CDM, OPM has employed automated continuous security features including greater visibility and accountability of asset management, device quarantine, asset management baseline, VPN enforcement, scheduled and automated patching, security agent compliance checks and enforcement, and USB blocking.
- There are additional organizational benefits by using CDM. It gives system owners a physical presentation of the risk of their system and fosters communication and collaboration between IT departments.
- The CDM program potential includes dashboard integration to better explain the risk to the system and expanded use of tools.

Any time you have disruption, you have an increased risk. Security threats are the biggest disruption to the workplace.

MONITORING TECHNOLOGY

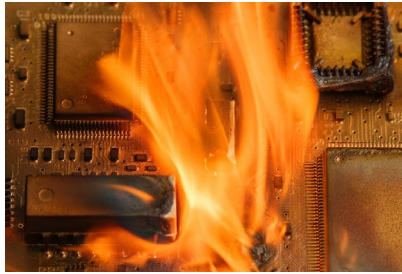
IT Glitch at NASA Led to Fire

A security patch that shut down monitoring equipment in a large NASA engineering oven resulted in a fire that destroyed spacecraft hardware inside. Since the computer reboot to accommodate the software upgrade also crippled fire alarm activation, the fire in the oven wasn't discovered for three and a half hours. This is just one example of how a lack of coordination between IT and industrial control systems can wreak havoc, according to a Feb. 8 report from the space agency's inspector general.

NASA has been automating many of its isolated, manually controlled technologies in favor of more sophisticated and interconnected IT equipment. But the agency's approach to integrating cyber, IT and physical systems is still a work in progress, and gaps in standards, training and security best practices need to be remediated, according to the OIG.

In other words, NASA's approach to the security of interconnected control systems is "reflecting society at large," according to the report. The details in the report show that NASA is suffering some of the same coordination problems and unintended side effects that have cropped up at companies and agencies mixing their manual operational technology for infrastructure systems with IT systems.

According to the OIG, 65 percent of the agency's critical infrastructure—including environmental monitoring and control systems that control heating, cooling, ventilation, power, rocket propulsion testing systems, spacecraft and aircraft command and control systems—are managed and supported by OT, or hybrid OT/IT systems.



candidate Paul Ryan (R-Wis.) during Mitt Romney's 2012 bid.

During his time in Congress, Lira developed a reputation for innovation. He organized the first Congressional Hack-a-thon on ways to improve the legislative process, helped build relationships with Silicon Valley and launched the phone app YouCut, the first digital platform directly linked to House floor votes. The app provided users the chance to hold their own weekly vote on proposed government cuts to be considered by House Republican leadership. He will join a White House tech team that includes deputy chief technology officer Michael Kratsios, the former top aide to Trump transition team member Peter Thiel. Trump has yet to name a chief technology officer.

CYBERSECURITY POLICY

Rare Good News for Federal Cybersecurity

At a time when government networks are increasingly under attack—and government itself is being criticized for not doing enough to respond—the recent award of the Credentials and Authentication Management task order of the Department of Homeland Security's Continuous Diagnostics and Mitigation program is a welcome piece of good news.

CRED, like other components of phase 2 of the CDM program, focuses on identity and access management, which has been a sore point for most government systems. Consider every major U.S. government breach of the last five years—whether by insiders such as Chelsea Manning and Edward Snowden, or by foreign adversaries as we saw in the attack on the Office of Personnel Management—has taken advantage of inadequate identity solutions and

TECHNOLOGY AND POLITICS

White House Adds a Tech Adviser

The White House has reportedly hired a veteran Republican strategist to serve as a technology aide to President Donald Trump. Matt Lira, most recently the senior advisor to House Majority Leader Kevin McCarthy (R-Calif.), will become the special assistant to the president for innovation policy and initiatives. The story was first reported by Recode.

Lira, who became a Harvard Kennedy School fellow in 2015, has experience in both chambers of Congress, as well as on the presi-

dential campaign trail. He served as the deputy communications director—and later digital director—for former Rep. Eric Cantor (R-Va.) from 2006 until 2011. When Cantor became House Majority Leader in 2011, Lira was tapped as his senior advisor.

In March 2013, he briefly left the House to become the deputy executive director of the National Republican Senatorial Committee during the 2014 midterm cycle. Lira returned in July 2015 to his former position of senior advisor to the House Majority Leader, this time for McCarthy. Lira also served as the webmaster for Sen. John McCain (R-Ariz.) during the 2008 presidential campaign, and was the digital director for then-vice-presidential

used them as the vector of attack. In some cases, it was a compromised password, but in other cases, it was someone who had a legitimate credential and was able to use it in ways that should have never been permitted.

Last year's report from the White House Commission on Enhancing National Cybersecurity highlighted our cyber identity problems, stating, "Identity, especially the use of passwords, has been the primary vector for cyber breaches—and the trend is not improving despite our increased knowledge and awareness of this risk." The report went on to say that "an ambitious but important goal for the next Administration should be to see no major breaches by 2021 in which identity—especially the use of passwords—is the primary vector of attack."

There are two areas of good news here with regard to CRED: First, the newly awarded CRED solution is delivering capabilities to agencies that will serve as the cornerstone of a "Five As" approach. CRED is focused on managing credentials and authentication. Second, DHS and the General Services Administration somewhat craftily negotiated the award of the CRED solution — choosing a solution that does not just "check the box" on meeting the CRED requirements, but that also gives agencies the option of apply-

ing some "bonus" features.

Congress has already put ample funding behind the CRED solution, covering the costs for all civilian agencies to deploy it. Agency executives should now look to take advantage of that funding, both to upgrade their IAM systems to guard against the full range of identity-centered cyberattacks and to enable new efficiencies in the way they do business.

TECHNOLOGY ACQUISITION

GSA Looks to Streamline Cyber-buying

Agencies will have access to products approved for a key federal cybersecurity program under the government-wide Schedule 70 contract vehicle thanks to a new acquisition strategy being rolled out by the General Services Administration. GSA proposed a new special item number (SIN) for Continuous Diagnostics and Mitigation program tools that give agencies access to approved network monitoring products and services. The CDM program is jointly administered with the Department of Homeland Security. The move comes as the August 2018 expiration of CDM's blanket purchase agreement looms.

Jim Piche, sector director at GSA's Federal Systems Integration and Management center, said the new Schedule 70 SIN will play a big role as DHS and GSA gear up for Phase 3 of the CDM program, and ensure that all the work done to approve and catalog products and services for the current BPA isn't lost when that contract expires. That product list contains "over 169,000 tools," he said.

GSA is moving relatively quickly on the successor acquisition vehicle. The request for information for the phase three contacting has been out since last fall, but the agency plans an industry day in April to explain how it is proceeding and issue a request for quotes that will be due back this summer, said Kevin Cox, the Department of Homeland Security's CDM program manager. Cox said GSA hopes to make the first phase 3 awards beginning in fall of 2017 and continuing into next year.

The current BPA, Piche said at a March 23 cybersecurity conference in Washington by FCW, don't give agencies flexibility in the kinds of contracts they can use to implement CDM. Additionally, the agreements limit agencies' ability to add in new technologies and accommodate changes. The new approach leverages the power of large-scale task orders to government-wide contracts instead relying on only BPAs.

"Identity, especially the use of passwords, has been the primary vector for cyber breaches."

—WHITE HOUSE COMMISSION ON ENHANCING NATIONAL CYBERSECURITY

CYBERSECURITY POLICY

DHS Cyber Reorg Bill Coming

The chairman of the House Homeland Security Committee plans to reintroduce legislation that would rename and reorganize the cybersecurity division at Department of Homeland Security in the coming weeks, dubbing it a priority. The Department of Homeland Security has been touting a plan for some

time to reorganize and rename its National Protection and Programs Directorate to more closely bind cyber and physical security capabilities as well as elevate the directorate to a headquarters division.

In a March 28 subcommittee hearing on the current state of DHS' effort to secure federal networks, House Homeland Security Committee Chairman Michael McCaul (R-Texas) said he will introduce a bill in the next two weeks that would "create a stronger, consolidated cybersecurity agency" at DHS. The proposal, he said "will elevate the cybersecurity mission at DHS at a critical time and further enhance cyber operations, including those to more effectively secure federal networks." McCaul told FCW after the hearing that he planned a markup of the NPPD bill "by the end of spring" and that it was a priority.

In testimony before the Cybersecurity and Infrastructure Subcommittee, Jeanette Manfra, acting undersecretary for cybersecurity at NPPD, told lawmakers that rebranding the agency was at the top of her legislative wish list. "It's very important for us," she said. Lawmakers on the panel asked Manfra about the progress of DHS' Einstein, Continuous Diagnostics and Mitigation and information-sharing programs.

DHS came in for only slight criticism on Einstein and CDM shortfalls during the hearing. Gregory Wilshusen, director, Information Security Issues at the Government Accountability Office, said Einstein was limited in its ability to detect intruder signatures that weren't on its list or hadn't been detected before. Its ability to analyze network data for trends as well as share information with agencies on cyberthreats and incidents were also limited.

Manfra said a year into the threat indicator sharing program, there are about 200 participants getting indicators from DHS. "We're looking to improve the program," she said, potentially providing scoring and

context along with the indicator data. She said companies "understood that we're improving, but we still need to do more."

PUT CDM INTO PRACTICE

Getting Agencies Access to Insider Threat Solutions


The problem of insider threats is so prevalent that the General Services Administration issued a Schedule 70 special item number for Continuous Diagnostics and Mitigation products and services after having jointly set up a CDM contract with the Department of Homeland Security. Bloomberg Government recently issued a study that pegged CDM as a \$1 billion opportunity for contractors and listed top providers and the contracts being used. While that study focused on the industry perspective, it contained valuable insights for government as well.

With agency IT departments under constant pressure on several cyber fronts, federal IT managers often need quick access to the best solutions to combat each threat. The Bloomberg study shows the preferred contract vehicles for

acquiring CDM tools and services, and these are often government-wide acquisition contracts—especially the NASA SEWP program—or other indefinite delivery, indefinite quantity contracts. Other vehicles include the GSA/DHS CDM contract; GSA's Schedule 70 and 8(a) STARS; DHS' First Source II and EAGLE II; the Department of Veterans Affairs' T4, the Centers for Medicare and Medicaid Services' Enterprise System Development; and NITAAC's CIO-SP3 from the National Institutes of Health.

The BGov study covered the period of 2012-2016, and while the usual large contractors (Booz Allen, HPE, and others) were on the leader list, small business contractor Sword & Shield led the CDM vendors, posting over \$531 million in CDM-related sales to the federal government over the five year period. Further, 99 percent of Sword & Shield's CDM-related sales went through NASA SEWP.

On the Sword & Shield blog, VP of Federal Raymond Kahre states, "Whether by accident, negligence or ill intent, insider threats present a real danger to federal agencies and battling them requires an intentional approach. At Sword & Shield Federal, we partner with government and industry to design and implement the right solutions to minimize the risk that insider threats pose to agencies."



With agency IT departments under constant pressure on several cyber fronts, they need the best solutions to combat each threat.

Kentoh/Shutterstock.com