Continuous Diagnostics and Mitigation (CDM) and Einstein:

The Foundations of Federal Civilian Cyberdefense

Contents

Executive Summary

Interest in government cybersecurity has never been higher. High-profile insider leaks by Edward Snowden and Chelsea Manning, coupled with external attacks on entities including the White House, have attracted a spotlight. But after data on 21.5 million federal employees and their families was exposed in breaches of the Office of Personnel Management's information systems, many more people were left asking how and why.

Those questions are not going unanswered. The government has taken swift action in response to the hacks. One step is to expand and accelerate the government's $6 billion Continuous Diagnostics and Mitigation (CDM) program. Established by the Homeland Security Department to help federal civilian agencies and departments plus state, local regional and tribal governments boost cybersecurity for unclassified networks, CDM provides services and tools that automatically detect and report on known cyber flaws or vulnerabilities.

In a July speech at the Center for Strategic and International Studies (CSIS), DHS Secretary Jeh Johnson called for the department to make CDM available to 97 percent of the federal civilian government – a goal that has already been exceeded, with 98.7 percent of executive branch agencies now involved in the CDM program, said Mark Kneidinger, Director of DHS' Federal Network Resilience (FNR) Division during an Oct. 20, 2015, GovLoop event. Johnson also asked Congress to authorize funding to speed the subsequent phase of the three-phase CDM.

Federal Chief Information Officer Tony Scott, also stepped up, calling in June, soon after the OPM hack was revealed, for a 30-day cybersecurity sprint that asked federal departments and agencies to:

- "Immediately deploy indicators provided by DHS regarding priority threat-actor Techniques, Tactics and Procedures to scan systems and check logs;"
- Patch critical vulnerabilities;
- Tighten policies on access for privileged users, especially by minimizing the number of them and limiting their functions;
- Apply multifactor authentication by requiring the use of a Personal Identity Verification or other smart card, not just username/password login combinations.

As a result of the sprint, 72 percent of agencies increased their use of multifactor authentication, up from 42 percent, and 13 agencies — more than half of the largest ones — increased usage of multifactor authentication to almost 95 percent of their privileged users.

It's a start, but not enough, Scott wrote in a blog post.

"To accelerate and amplify the work and objectives of the Sprint, a team of over 100 experts from across the government and private industry are now leading a review of the Federal Government's cybersecurity policies, procedures, and practices," he wrote. "Ultimately, the team's assessment will inform and operationalize a set of action plans and strategies to further address critical cybersecurity priorities and recommend a Cybersecurity Sprint Strategy and Implementation Plan to be released in the coming months."

These fixes are great, but what's really needed is a cybersecurity overhaul, say experts such as Richard Spires, Chief Executive Officer of Resilient Network Systems and former CIO at DHS. As the threat surface expands because of the proliferation of mobile devices and the Internet of Things, the threat surface multiplies in size, and these growing technologies have made the traditional cyber approach – perimeter defense – less effective because the boundary is not so concrete anymore.

"I have thought for a while that really what we need to do is work much harder on protecting that information directly and swing our resources more to doing that, and less to trying to protect all of our systems – the old perimeter concept," Spires said. That way, data would be protected regardless of where it resides.

Moreover, with each agency and department holding responsibility for its own cybersecurity plan, the risk of silos runs high. Agencies aren't on the same page in terms of protection or threat information sharing, which is a danger because when one system is compromised, other agencies need to know. Knowledge can help them know what signs to look for so they can turn an attack into an attempt.

The fact is there is no silver bullet that can make cyberspace and data 100 percent secure.

"I think we're constantly looking for areas where we can continue to improve and grow and mature," said Ann Barron-DiCamillo, Director of the U.S. Computer Emergency Response Team (US-CERT). "Cyber is a relatively immature industry, and it's constantly evolving at light speed. Having it not be as mature as some other industries in a very volatile state and the speed at which things change and we're government so we don't always change and evolve as quickly as our industry does. It's definitely a challenge, but I think we have a lot of important support from not only Congress, but from the White House, this administration, as well as key stakeholders across the community, both domestically and internationally."

DHS developed two programs to significantly bolster federal cybersecurity and create a baseline standard: CDM and Einstein, a $3 billion intrusion-detection system that has become much more. To ensure these efforts continue to help defend against cyber threats, President Obama's fiscal 2016 budget invests $582 million in CDM and Einstein.

In this guide, we will look at:

- What CDM is, how it works and what it entails
- What Einstein is, how it works and what it entails
- Steps to increasing cybersecurity and how these programs play a role
- CDM and Einstein best practices
- What's next for federal cybersecurity

Before we can understand the programs' evolution, we must understand what they are and where they came from. Let's start with CDM.

Continuous Diagnostics & Mitigation: A Refresher

Here's how CDM works in a nutshell: DHS evaluates and buys commercial IT security tools and services that aid in the continuous diagnostics and mitigation processes of federal civilian agencies' networks and systems. Those agencies can then procure those products and services via the General Services Administration, which partnered with the department to set up a government-wide acquisition vehicle for this purpose.

The word diagnostics means a symptom or characteristic or the practice or techniques of diagnosis. In terms of CDM, this means monitoring or watching unclassified networks for known cyber flaws or vulnerabilities on a continuous basis. DHS defines CDM as "a dynamic approach to fortifying the cybersecurity of government networks and systems." CDM does this by providing tools that let agencies identify cyber risks on an ongoing basis and prioritize them based on potential outcomes. Using that information, personnel can mitigate the most significant problems first, the department said.

"Congress established the CDM program to provide adequate, risk-based and cost-effective cybersecurity and more efficiently allocate cybersecurity resources," according to DHS.

To get the tools and capabilities to agencies, DHS partnered with the General Services Administration to create a blanket purchase agreement that provides automated security tools and services for agencies to buy. Although the idea is for agencies to procure what they need at reasonable prices, DHS-appropriated funds also offset the costs to agencies.

CDM supports federal cybersecurity by helping agencies install commercial off-the-shelf (COTS) tools that work in a six-step process that scans all systems within 72 hours:

1. Agencies install sensors on their networks.
2. The sensors automatically search for and detect flaws.
3. The sensors' results feed into a dashboard.
4. The dashboard analyzes the data and creates customized reports that can alert network administrators to problems.
5. The tool assigns weighted scores to the sensors' findings so that admins can prioritize their responses.
6. The dashboard generates progress reports so agencies can adjust resources according to risk.

Additionally, a summary can be sent to an enterprise-level dashboard that can inform situational awareness government-wide, knocking down some of those silos we mentioned earlier.

CDM has three phases covering 15 continuous diagnostics capabilities, which are defined by the National Institute of Standards and Technology as sets of security controls that work together. Here's how DHS describes them:

Phase I:

This is the basic level at which agencies are installing sensors and gathering information. It also helps IT managers inventory their hardware and software so that they can prioritize their assets. Jim Quinn, Lead System Engineer for CDM, broke it down like this during an Oct. 8 GovLoop webcast titled "CDM: Securing the Data, Not Just the Perimeter":

- **Hardware asset management** – what assets the agency has, which are valid and what risk is associated with each one.
- **Software asset management** – what assets the agency has, ensuring that what's installed is legitimate and tracking who authorized the installation.
- **Configuration settings management** – establishing baselines and measuring compliance with them.
- **Vulnerability management** – scoring vulnerabilities so that administrators know how to prioritize mitigation.

Phase II:

At this stage, the focus shifts to infrastructure integrity and the principle of least privilege, which states that eliminating unnecessary user privileges based on job necessities can reduce vulnerability, according to Indiana University. In other words, Quinn said, this stage is about not just knowing what's on your network, but who's on your network and what characteristics they have.

- **Access control management in the form of trust** – making sure managers have conducted background checks on users.
- **Security-related behavior management** – policy and training compliance, including having signed nondisclosure agreements and rules of behavior in order.
- **Credentials and authentication management** – including credential types and security levels.
- **Privileges** – what users are allowed to access.

Phase III:

This tackles event management, boundary protection and security lifecycle. It's about building perimeter controls and knowing what to do with them, focusing on networks instead of endpoints, controlling physical access and using encryption to protect data at rest and in transit, among other details, Quinn said.

- **Plan for events** – building and using perimeter controls and setting physical access control systems. This also includes planning for encryption, protecting data in transit and at rest and managing keys and certificate authorities.
- **Respond to events** – being able to execute contingency plans if networks go down or if there are security incidents such as improper use of data.
- **Generic auditing and monitoring** – maintaining information so that you can validate it and have records of events.
- **Document requirements, policy and more** – determining how to do security planning and how to build secure code.
- **Quality and risk management** -- administrators can make better risk-based decisions using the information they have about their asset inventory and their understanding of network vulnerabilities.

"Once fully deployed, CDM will monitor agency networks internally for vulnerabilities that could be exploited by bad actors that have breached the perimeter," DHS Secretary Johnson told Center for Strategic and International Studies. "CDM will allow agencies to identify, prioritize and fix the most significant problems first. It will also provide DHS with situational awareness about government-wide risk for the broader cybersecurity mission."

How to Get CDM

Federal civilian agencies, state, local and tribal government agencies may purchase CDM tools through GSA's CDM blanket purchase agreement (BPA). The Federal Acquisition Regulation established BPAs under GSA Schedule contracts to serve as "charge accounts" with trusted suppliers to "simplify the filling of recurring needs for supplies and services, while leveraging ordering activities' buying power by taking advantage of quantity discounts, saving administrative time, and reducing paperwork," according to GSA. With CDM, participating agencies save money through GSA Multiple Award IT Schedule 70 pricing and tiered discounts based on cumulative quantities.

As of Sept. 11, the CDM Tools/Continuous Monitoring as a Service (CMaaS) Product Catalog included companies offering products for phases I and II. BPAs have been awarded to 17 contractors so far. According to the 2015 Ordering Guide, the performance period of the multiple-award CDM Tools/CMaaS BPA is five years — a one-year base period and four one-year options.

"It is not just a technology program bringing a set of products together to be made available across the government," Quinn said. "It actually has been formulated by Congress and by the appropriation that came from Congress to really fix what is usually viewed as the major problem in government, which is we don't have a responsive procurement system, and with cyber threats coming at us so quickly, we needed to have something that's much more adaptive and responsive."

CMaaS has 11 service task areas that contractors must meet:

- **Support of order project management**, including providing project schedules, monthly status reports and all necessary staff and financial resources
- **CDM order planning**, which includes plans for the company's approach to implement the CDM capabilities set out in the order and participation in technical design reviews
- **Support of CDM dashboards**, meaning the contractor must be able to install, configure and maintain dashboards related to CDM
- **Provide specified tools and sensors**, which may support functions such as hardware or software inventory management, configuration setting management and credentials and authentication management
- **Configuration and customization of tools and sensors**, which means contractors must meet agencies' specifications
- **Maintenance of data** on desired state for CDM tools and sensors, which means information stays current
- **Operation of CDM tools and sensors**
- **Integration and maintenance of interoperability** between CDM tools and legacy applications and data
- **Operation of data feeds** to and from installed dashboards
- **Training and consulting** in CDM governance for agencies and other requesting organizations to help establish an overall cybersecurity governance program
- **Support of independent verification and validation and system certification**, meaning that contractors will help third parties evaluate their tools and services

Three order types are allowed under the BPA. The first is called labor hour, which is used to cover projects with labor only. The others are cost-reimbursable, meaning that only travel portions of any GSA Schedule order can be reimbursed, and firm-fixed price, which is recommended for commodity tool procurements and services procurements.

"Each Task Order/Delivery Order under the BPA can have a combination of contract types (e.g., LH for Labor, FFP for products and CR for Travel)," the ordering guide states.

"We can't solve all the problems with federal acquisition in a program of our size, but we can make sure the latest technology is evaluated, reflected in our formal statements of work to industry and ultimately reflected in the products and services on the General Services Administration Schedules of the Continuous Monitoring-as-a-Service providers," former FNR Director John Streufert said in an April interview with Federal News Radio.

A CDM Timeline

January 2014

First Phase I task order awarded for $60 million under CMaaS for hardware and software inventory tools, software licenses and products to provide immediate protection for network endpoints such as desktop computers and servers

February 2015

$29 million contract for Task Order 2 Group A awarded for a vulnerability manager, e-policy management tools, a network access control tool and big-data analytics software

April 2015

$39 million contract for Task Order 2B, for the departments of Energy, Transportation, Interior, Agriculture and Veterans Affairs and the Office of Personnel Management, awarded July 2015. DHS Secretary Jeh Johnson asks Congress for funds to accelerate Phase II

September 2015

Three more task orders awarded, worth about $140 million, bringing CDM tools and services to 17 more federal civilian agencies and covering 97 percent of them

Fiscal 2016

Delivery of Phase II expected

Fiscal 2017

Delivery of Phase III expected

Printer security breach?

Not on your watch.

Defend your network with the world's most secure printers.

New enterprise HP LaserJets with JetIntelligence provide the industry's deepest printer security.[1] Features including HP Sure Start with its self-healing BIOS, whitelisting, and runtime intrusion detection come built in.

hp.com/go/printersthatprotect

[1]The world's most secure printers and deepest level of security: Based on HP review of 2015 published embedded security features of competitive in-class printers. Only HP offers a combination of security features for integrity checking down to the BIOS with self-healing capabilities. Available on the HP LaserJet M527, M506, M577 and as an upgrade on the M552, M553, M604, M605, and M606. Some features will be made available as a HP FutureSmart service pack update on selected existing Enterprise printer models.

[2]Ponemon Institute, "Annual Global IT Security Benchmark Tracking Study," March 2015.

Industry Spotlight

Addressing the Critical Issue of Printer Security

An interview with Shivaun Albright, Distinguished Technologist, HP

Continuous monitoring (CM) enables agencies to constantly assess their IT security risk posture from all levels of the organization. It provides current security and compliance insights in real-time, to help improve security situational awareness and make cost-effective risk-based decisions.

Continuous monitoring and cybersecurity are more important than ever, and government agencies are making real strides in many ways to make their data safer.

One area of security that is often ignored is printers used in government agencies.

Looking at a basic printer, you might not view it as a possible launch point for a hacker looking to get onto your network. But the fact is that it's actually extremely vulnerable. GovLoop sat down with Shivaun Albright, Distinguished Technologist, HP, to discuss how government can address this security need.

"Printers are essentially an endpoint on a network," Albright explained. "Customers invest in endpoint security for their PCs, and their routers, etc. But the printing side of it is often overlooked. We're trying to educate customers that every endpoint should be an equal citizen on the network."

Albright's point was that most agencies invest in policies for securing computers, mobile devices, antivirus scanners, and making sure patches on their operating systems are up to date.

"But we're seeing that customers are often overlooking their printers," Albright said. "However, printers are just as critical."

When you attach a printer to your network without configuring that device, Albright explained, the device becomes a potential attack vector to hackers. And once they can access the device, they may launch an attack from that device to target other endpoints on the network.

In fact, an average printer today has over 250 possible security settings. And as with all manufacturers, whether it's PCs, desktops or printers, the device comes to a customer not configured and potentially vulnerable. So it's important that administrators set security policies to bring those devices into compliance with their organization's endpoint policies and make sure that their printers are locked down in a similar way to their PCs.

"HP is committed to security, and it's been a journey." Albright said. "We provide the tools, solutions and device hardening capability to protect our customer's environment and their data."

HP has recently focused on adding layers of security to their devices to provide a defense-in-depth mechanism that can help detect when somebody is trying to attack the system.

"Hackers are known for finding weak links on any device," Albright said. "What we've done primarily is to make sure devices are running the intended code that should be run. We're validating that the firmware used hasn't been tampered with, and ensuring that the code came from HP."

Additionally, HP now offers a printing security advisory service.

"We provide the customer with education on security threats and analysis of the current printing security posture," Albright explained. "We do an assessment of their devices using a tool called JetAdvantage Security Manager that assesses a customer's fleet of devices, and identifies where a printer has potential issues or vulnerabilities because they're not configured properly."

HP developed the JetAdvantage Security Manager tool with default/recommended printing security policies based on industry best practices and internal expertise. The service provided by HP features an assessment of the customer's fleet security posture. Once HP completes the fleet assessment, the security advisor helps the client build a comprehensive printing security policy that meets their business needs as well as their best practices.

"We'd like to see more awareness of the risks of printing and imaging devices, as well as an increased focus on device security," Albright said. "Looking forward, we'd like to see a better integration of print device security with cloud services. That area is growing significantly. We expect to see more integration into cloud services, cloud offerings, either private or public clouds, that allow workflows to and from our printing and imaging devices."

In short, agencies need to work to build a strong printing security policy that lets them secure and continuously monitor print endpoints, add advanced solutions such as authentication, and deliver print services like secure printing, mobility and workflow.

Where CDM Stands Now

CDM, which is expected to take five years to implement, is currently in Phase I. As of February 2015, agencies had procured more than 1.7 million licenses for asset, configuration and vulnerability tools, according to the Office of Management and Budget's (OMB) FISMA report to Congress.

In September, DHS awarded three task orders that increased the availability of tools and services to 17 more federal civilian agencies. This move achieved the goal Johnson set in July, when he called on the department to make CDM available to 97 percent of all federal civilian agencies. The contracts, worth almost $140 million, marked three of six awards under the CMaaS BPA.

Additionally, smaller or micro agencies are signing memoranda of agreement to use CDM following an OMB memo last October that gave DHS the authority to regularly scan federal agency networks.

Also in July, Johnson called on Congress to authorize funding to accelerate Phase II, which is slated for delivery in fiscal 2016. In June, Federal Times reported that DHS was starting to look at the first task orders for Phase II, the one focused on identity, credentials and access management. And things should move more efficiently from here on out: "Once agencies have the base scanning and monitoring capabilities of Phase I, incorporating strong authentication controls should be easier," according to the article.

"The BPA has been structured so that each of the phases is an add-on to the prior phase," Jim Piche, Federal Systems Integration and Management Group Manager for CDM, told Federal Times.

As the push for Phase II continues, the CDM program is starting to implement the agency and governmentwide dashboards, which are for continuous risk-assessment and information-sharing.

"As the awards are made for Phase I, the vendor or awardee will then also be working in regards to moving the dashboard into those agencies," Kneidinger told Federal News Radio in June 2015. "Where we are with the dashboard is at the department and agency level, we are looking at this juncture of Q3 of 2015 for the department/agency dashboard to be moved into the first set of agencies under the various awards and in the sequence of awards."

Kneidinger added that DHS and OMB will launch the federal dashboard in the first quarter of 2016. "Vendors will connect the agency level dashboards to the federal dashboard to feed data and trends," according to Federal News Radio.

What's more, CDM is making use of DHS's Leap Ahead Technologies program, which "is focused on identifying, incubating, and executing early research projects that may significantly advance current capabilities through moderate risk and high-payoff outcomes," according to DHS.

Before he retired earlier this year, Streufert told Federal News Radio that DHS was reviewing the technologies in the program to see what might help CDM.

Shortly after his retirement, CDM program management shifted from FNR to the Network Security Deployment division, whose mission is to serve as the cybersecurity engineering and acquisition Center of Excellence within the Office of Cybersecurity and Communications (CS&C). FNR is another division of CS&C.

Despite these forward movements, 58 percent of federal CIOs see CDM as simply "a tool in the toolbox," according to a 2014 Federal News Radio survey. Still, 80 percent said it will improve their agency's cybersecurity.

Part of the holdup is the lack of an overarching cybersecurity organization, some experts suggest. Each agency is responsible for its own cybersecurity, making each implementation of CDM tools unique. That takes time to set up.

"While DHS is speeding up deployment of our current tools and developing new approaches, cybersecurity is inherently a shared mission," said Andy Ozment, Assistant Secretary of CS&C, in a September GovTech interview. "Every federal agency and private-sector company has a key role to play — to understand their own risk, implement best practices, participate in information sharing activities and effectively respond to cybersecurity incidents. At DHS, we stand ready to help our partners in effectively managing their cybersecurity risks and adapting to threats that are increasingly a condition of our networked lives."

> *"Every federal agency and private-sector company has a key role to play — to understand their own risk, implement best practices, participate in information sharing activities and effectively respond to cybersecurity incidents."*
>
> *- Andy Ozment, Assistant Secretary of CS&C at DHS*

Use of CDM is a critical tool to shrinking or at least better managing the threat surface, said US-CERT's Barron-DiCamillo.

"That tool will enable departments and agencies to implement a lot of the top controls that we've been touting as far as helping respond to incidents that we've seen," she said. "So with the use of CDM, departments and agencies can implement the capabilities they need to protect their high-value assets and their sensitive data and their [personally identifiable information], and it will also help them monitor. Things change and evolve in your environment. You need to continually monitor for those changes and ensure that your tools are keeping up with the evolution of cyber. And CDM will enable them to implement and then continue to monitor and then make those adjustments as things are evolving and changing."

SPOTLIGHT:
Q&A with John Simms,

CDM Program Manager & Requirements and Acquisition Support Branch Chief, DHS

To get a handle on where the CDM program has been and how far it has yet to go, we went straight to the source: Program Manager John Simms.

How has CDM evolved since its inception?

CDM began in the fall of 2012 and a lot of things have changed. The general strategic view of CDM and the vision that John Streufert brought into DHS with regard to CDM hasn't changed, but what has changed is the level of participation and engagement by the departments and agencies in the federal civilian sector. We went from [having] back in 2012/2013 a commitment to Congress of five agencies participating in the program and we now have all 23 [Chief Financial Officers] Act agencies as well as over 40 small and micro agencies. So, that's one aspect that's changed.

The other aspect that's changed is over the course of time, we've seen a great deal of interest in the program by the federal civilian community in terms of their willingness to participate in the program and participate at a level that provides them with the ability to engage directly in our acquisitions as well as doing the evaluations of the acquisitions supporting their agencies. So, we view that as a positive sign.

In addition to that, on our BPA, we have a ton of COTS products supporting the security capabilities that we're deploying with CDM, but one of the aspects of the program from 2012 concerning the dashboard capability for CDM was back then we were under the impression that it might be difficult to get a COTS product to support our requirements for the dashboard, and we were looking at the possibility of having to develop the CDM dashboard in house or contract it out. Through the contract we have with Metrica Team Venture, we were able to do an analysis of alternatives based on our requirements, and there were several capabilities to support our requirements in the commercial sector, so that's one major aspect of something that's evolved since the start of the program.

Is CDM keeping pace with the evolution of technology?

Right now we're in the process of deploying Phase I capabilities through our Task Order II capability.

I would say that the capabilities that we're deploying are somewhat ubiquitous in terms of they've been on the market for quite some time and there are some aspects that are newer in terms of the technology. In terms of our Phase II capabilities that we're deploying, that's centered around identity management, credential access management – those are somewhat newer, but I would say that we are definitely keeping pace with the evolution of technology. Up until a couple months ago, we had an active engagement with industry through what we call our Leap Ahead technology, and basically what we were doing is a separate organization within the Federal Network Resilience Division was engaging directly with industry on cutting-edge cybersecurity technologies that could be used not only as a method of making DHS aware of some of the new technologies out there, but also if there was an interest by the BPA teams, making introductions through the GSA so that those technology vendors could talk with the BPA teams on the DCM CMaaS BPA to see if they would be a good fit for our program.

Is CDM being adopted quickly enough?

That's an interesting question, because quickly enough in the cyber world is not fast enough. We've been actively engaging with departments and agencies on a very regular basis since 2013, and I can tell you that we're all moving as quickly as we can. One of those challenges is the federal acquisition process requires a particular process, which is respected by the program and the departments and agencies. I think if you look at what we've done in the last 18 months with regard to our Task Order II activity and our Delivery Order I activity, we've moved very quickly. Coalescing the requirements from 23 CFO Act agencies and we've been engaging with small and micros for the last six months and getting the requirements together and put in solicitations and getting bids from industry and then evaluating those bids, we've moved very quickly. We'd all like to move much faster, but we all understand what we have to do as program managers and project managers and acquisition professionals to ensure that there's integrity in our processes and a level playing field for industry.

Are there other challenges that aren't related to acquisitions, perhaps workforce shortages?

Generally, all federal agencies are challenged with having adequate levels of staffing with cybersecurity and information security profession. I think that's not only a government issue, that's also an issue for the private sector. Our private-sector partners typically have the ability to structure their compensation a little bit differently than the federal agencies can. But I would say there's just a general shortage of skilled professionals out there. We've got a great mix of them within the federal community and we are leveraging them to the greatest extent possible, but quite honestly, I would say that one of the biggest obstacles is the complexity of the federal enterprise and networks within some of these agencies — they're enormous. We're working through the processes and change management aspects. To get our projects into their operational environment requires a lot of planning, a lot of planning that has to occur post-award. Once our awards are made, we immediately start communicating and engaging with the agencies and the contractors so that we can begin the preparation so that we can employ these technologies on their networks, but it does take time and we do have to follow the processes to ensure that it's done in a methodical way.

Is there an average amount of time it takes?

Not really. Because of the size and complexity of the networks, in addition to the mix of agencies that we have in each of the groups, it varies. Some agencies can move a little bit faster than others. When you have a federated organization, and there are many out there, that adds a level of complexity on top of an agency that may be a little bit more homogenous. But again, we have to work within the operational realities of those agencies and engage with them to get through their processes down to the component level at times to support the deployment of these technologies.

What about state, local, regional and tribal governments? Will CDM expand to apply to them?

Going back to the 2012 appropriation that Congress gave to DHS to start the program, it allowed DHS to provide CDM capabilities to federal civilian agencies, so intel and the Department of Defense is outside of the scope, as well as state and local governments. What we did, though, we worked with GSA [Federal Systems Integration and Management Center] to establish a blanket purchase agreement called the Continuous-Monitoring-as-a-Service blanket purchase agreement that is eligible to be used by state and local governments that can use federal acquisition vehicles. That's about the most direct way that we can support them in terms of bringing them technologies that we use in the federal community at a price point that's probably more attractive to them, given the buying power of the way in which the BPA is structured. So the larger the group that goes into an acquisition, the greater the discount is going to be on the orders.

What are you doing to push further adoption by federal agencies?

We continually engage with the departments and agencies through the [Information Security and Identity Management Committee] Council, which is under the federal CIO Council. [In October], we had one of our large presentations — typically those have been geared toward CDM specifically, but since the reorganization of FNR and the CDM program in particular into the Network Security Deployment division, CS&C under the direction of Andy Ozment and [Deputy Assistant Secretary] Gen. [Greg] Touhill, have provided us with an opportunity to direct outreach and support all of our cyber initiatives and offerings with CS&C and what we're doing is broadening that engagement with the federal community to include such other programs as Einstein in addition to CDM.

Are agencies and departments putting themselves at greater risk by delaying adoption of CDM?

That's kind of a tricky question. I don't know what the posture of a lot of these agencies are, but obviously if there are gaps in their technologies in terms of how well they can observe the security posture of their networks, then they would have a greater level of risk that they're taking.

Are there examples of CDM success stories?

I've got three in particular. I think one of the successes that we're recognizing is we're able to support the federal civilian security programs and filling in gaps in technologies that they've had for several years. So that's one thing that I'd consider a success. Greater coverage of their network is giving them greater visibility into issues that they can monitor and manage on a regular basis. That's one aspect.

The compliance aspect of FISMA and the manual nature of doing certification and accreditation or security authorizations is another thing that CDM is focused on. When we get our Phase I and Phase II and Phase III capabilities out in that order, we're going to be positioning ourselves as well as the rest of the federal government on the civilian side to automate the FISMA compliance aspects that have really – it's a major level of effort for what I would consider little gain in terms of those compliance activities are focused on a three-year cycle, whereas CDM is looking at within 72 hours assessing every device on the network, so we're looking at pushing this real time to the extent we can based on the agencies' networks, but that's a major aspect of this program: automating the testing of security controls leading to ongoing authorization.

The other is leveraging the buying power of the federal government. One example is on our first order back in 2014, it was a $60 million order — which was the largest IT Schedule 70 commodity buy performed by GSA, and we have a $26 million cost avoidance on that based on IT Schedule 70 pricing. That to me is a huge success. We're able to deploy these technologies and support the federal government and save the taxpayers a lot of money in the process.

What are some best practices for adopting and using CDM?

Focus a lot around planning. Planning in terms of where they were at before we started engaging with them, post-engagement with CDM and knowing we're about to deploy on their networks. I would say planning and governance are two really big areas where agencies need to stay really focused in terms of looking at what we are doing now, what we have planned in the near future and within the next couple of years and really looking at how that's going to affect their ability to operate their security programs, maintain their security posture and looking at that capability and understanding what may or not be covered, if you will.

There are a lot of agencies that are doing a lot of stuff in the cloud now and doing a lot of bring-your-own-device and those two particular aspects of computing are outside the scope of what we're doing with Task Order II – not to say we won't cover it in the future. I would say that planning is a big part of a best practice.

Furthermore, I would also say making sure they have adequately trained staff. We're providing some training through the program, and we have training that's available on the US-CERT.gov/CDM portal, but making sure that agencies are allowing their personnel to stay well trained is another best practice.

Looking ahead, what can agencies expect in terms of challenges to cybersecurity in general and CDM specifically?

There are always challenges concerning cybersecurity. … We're tightly integrated into a lot of the overarching federal initiatives involving cyber. They're looking at CDM as a capability that can be relied on to fill some of the gaps that are occurring in the federal community with regard to information security, so we are moving as fast as we can. Obviously, we'll move as quickly as the agencies can move, knowing that we have contractors we're using to deploy a lot of this technology. I can tell you that the agencies have also expressed an interest to move as quickly as possible. I don't really foresee any problems with the deployment of the future phases of CDM.

How to Use CDM

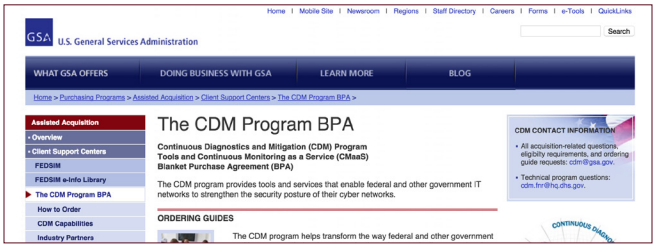
At 2 years old, the Continuous Diagnostics and Mitigation program is still fairly new, and as it starts to move into the second of its three phases, the federal civilian agencies that have signed on to use it might need some guidance on how to adopt and implement it. DHS, U.S. Computer Emergency Readiness Team and General Services Administration offer several resources for agencies embarking on or already using CDM tools and services.

US-CERT's CDM portal

This site offers information for government cybersecurity professionals who are getting started with CDM. It offers toolkits on the CDM hardware asset management capability, the configuration settings management capability and other Phase I aspects. The portal also offers training materials on implementations and ongoing assessments in addition to capability definitions and data sheets.

Federal Virtual Training Environment

This online, on-demand cybersecurity training resource offers a content library with pre-recorded classroom trainings for government employees and contractors. Courses range from beginner to advanced levels and are available for free from any Internet-enabled computer.



GSA's CDM blanket purchase agreement site

This webpage offers resources such as ordering guides, a product catalog and explanations of the program's capabilities. It includes a "how to order" link, and answers frequently asked questions about what CDM is and how it works.

merlin

secure.performance

BEATING PERSISTENT THREATS AT THEIR OWN GAME

Unified Cyber Forensics solutions from Merlin provide rapid discovery and remediation of even the most **Advanced Persistent Threats**.

Visit us at www.merlin-intl.com for more information.

Industry Spotlight

The Sweet Spot of Continuous Monitoring

An interview with Mark Zalubas, Vice President of Engineering for Merlin International

As cybersecurity has evolved into an arms race between hackers and protectors, continuous monitoring has quickly replaced periodic security posture assessments. But according to Mark Zalubas, Vice President of Engineering for Merlin International, a cybersecurity and IT solutions provider, many agencies are charging into these large efforts before fully understanding their unique characteristics and implications.

Continuous monitoring solutions generate a lot of data. It's analogous to your doctor outfitting you with a device that monitors your heart rate six times a minute instead of just once a year when you see her for a checkup. Agencies must be prepared to handle this massive influx of data.

According to Zalubas, different continuous monitoring solutions receive their deluge of data between two ends of a spectrum. On one end of the spectrum, there is the "fire hose scenario," where you have massive amounts of data rapidly and constantly delivered to your solution from a single location. Full network packet capture, or PCAP, solutions are an example of this end of the spectrum.

On the other end of the spectrum are solutions that receive small amounts of data from large quantities of devices. Governance, risk, and compliance, or GRC, solutions are an example of this end of the spectrum. Nevertheless, the end result is the same: "You are still dealing with a lot a data."

Agencies embrace new continuous monitoring technologies and their ability to deliver better insight and thus better protection. "But with a lot more data also comes a lot more storage, processing, bandwidth, configuration, and thus a lot more expense," said Zalubas. "These are complex solutions that are more challenging in configuration and performance than what most IT professionals have dealt with in the past."

For example, a PCAP solution on a 10 Gbps network tap could generate over 100 TB of storage per day. Likewise, a GRC solution in an enterprise with 500K endpoints must configure every one of those disparate endpoints to forward the required data within the desired periodicity. The attention to detail required to properly construct, configure, and instrument these solutions for continuous monitoring is high.

"But that is only half of the operational battle," Zalubas said. "The solutions aren't just there to collect data. You need to be able to make use of it too. You can't really buffer this cyber data and process it later, because collection never really stops."

The ability to scan, alert, query, analyze, and take action on the data is where real value is derived. The system must be designed to query data as it is continuously coming in, or contention for physical resources will reduce the solution's performance.

The complexity of analysis rules and correlation algorithms must also be considered. Data from these systems flow at rates that humans can't possibly keep up with, so automated rules must be configured to alert humans to only those events that are worthy of manual investigation. But, what do you look for? What correlation of firewall, antivirus, intrusion prevention cybersecurity events are concerning? What Windows misconfiguration should be immediately alerted? These rules must be coded and kept up-to-date within a constantly evolving IT infrastructure.

Zalubas advised, "Agencies should assess their overall cybersecurity posture and attempt to balance cybersecurity initiatives so that no one area receives too much attention and no area too little." He has encountered agencies trying to 'perfect' continuous monitoring solutions, unconscious of the fact that they have reached a point of diminishing returns. For instance, it doesn't make sense to store PCAPs for exceptionally long periods of if their valuable shelf life is days-to-weeks, especially if that means shorting another cybersecurity solution that isn't close to its point of diminishing returns.

Finally, Zalubas noted that many agencies are surprised by the challenge of continuous remediation. Continuous monitoring efforts are fruitless without the corresponding capabilities to remediate the flaws and vulnerabilities that the analysis uncovers. Continuous remediation can cost just as much, if not more, than continuous monitoring in technical and operational costs.

For most government organizations, balancing the demands of other enterprise functions with their efforts to craft a complex data architecture is overwhelming. That's why agencies like the Department of Veterans Affairs and the Department of Health and Human Services have turned to Merlin International for a variety of continuous monitoring and cybersecurity solutions.

Merlin's monitoring tools and expertise enable government leaders to gain deep insight into a continuous stream of near real-time snapshots of the state of risk to their security, data, the network, end points, and even cloud devices and applications to support better risk management decisions. As these myriad tools and technologies are applied, Merlin's engineers can also carefully integrate them into your current IT architecture and ensure the new data flows don't overload your agency.

Explaining Einstein

EINSTEIN is a program that detects and blocks cyberattacks from compromising federal agencies, as well as providing situational awareness to use threat information detected in one agency to protect the rest of the government. Here's what you need to know about it.

What Is it?

Let's begin with an explanation of the National Cybersecurity Protection System, operationally known as Einstein: "Einstein provides US-CERT a situational awareness snapshot of the health of the federal government's cyberspace," according to DHS. "Based upon agreements with participating federal agencies, US-CERT installs systems at their Internet access points to collect network flow data. The agencies are provided tools to analyze their collected data. In addition, the data is shared with US-CERT Security Operations Center, which aggregates it from all Einstein participants to identify network anomalies spanning the federal government."

In other words, DHS provides Einstein as a managed security service offering intrusion protection and prevention for civilian executive branch agencies. The department manages Einstein through its National Cybersecurity and Communications Integration Center. Like CDM, Einstein does not apply to the Defense Department and intelligence community.

And similar to CDM, Einstein has three parts, each adding to the capability of the previous iteration. DHS deployed the first – Einstein 1 – in 2004 to record and analyze network traffic to and from executive branch civilian agencies. It sits at the perimeter of agencies' networks and enables the department to spot suspicious activity and perform more detailed studies when breaches do occur.

Einstein 2 came out in 2008. It also sits at the perimeter, but it "identifies malicious or potentially harmful computer network activity in federal government network traffic based on specific known signatures," according to DHS. "In technical terms, it is an intrusion-detection system. On a typical day, Einstein 2 sensors generate approximately 30,000 alerts about potential cyberattacks. These alerts are each evaluated by DHS security personnel to determine whether they represent a compromise and if further remediation is needed."

Einstein 1 and 2 are fully deployed and screen all civilian executive branch traffic that is routed through a trusted Internet connection, or a secure gateway between each agency's internal network and the Internet. As a result, they are currently monitoring more than 90 percent of all federal civilian Internet traffic, DHS said, although Johnson said in July that they "protect all federal civilian traffic routed through a secured gateway to the Internet."

Those first two iterations apply only to unclassified information. Five years ago, DHS started work on a third version of Einstein that would be able to identify and block cyberattacks using classified signatures. In 2012, the department took a new approach — dubbed Einstein 3 Accelerated (E3A) — in which Internet service providers supply intrusion-prevention services using commercial technology. The initial deployment of E3A is focused on countermeasures that will address approximately 85 percent of the cybersecurity threats affecting federal civilian networks, according to OMB's February FISMA report to Congress. At that time, the DHS Office of Cybersecurity and Communications had deployed E3A at seven departments and agencies.

"The E3A program also serves as a platform to aggregate federal civilian executive branch traffic so that DHS can implement new and advanced protections," according to DHS. "In other words, by putting all federal government traffic through a few locations, DHS can easily add security tools to those locations. To this end, DHS is piloting protections that will automatically identify possible cyber attacks for further analysis, even if the precise attack has not been seen before. DHS is examining technologies from the private sector to evolve to this next stage of network defense."

DHS is providing at least one E3A protection to 17 federal civilian agencies, protecting about 45 percent of the federal civilian government, and has established memoranda of agreement with 55 federal agencies to implement E3A, according to the department. It will make basic E3A protections available to all federal civilian departments and agencies by the end of this year.

> *"Since its introduction, E3A has blocked over 550,000 requests to access potentially malicious websites. These attempts are often associated with adversaries who are already on federal networks attempting to communicate with their 'home base' and steal data from agency networks."*
>
> *- Jeh Johnson, DHS Secretary*

"E3A has demonstrated its value," Johnson told CSIS. "Since its introduction, E3A has blocked over 550,000 requests to access potentially malicious websites. These attempts are often associated with adversaries who are already on federal networks attempting to communicate with their 'home base' and steal data from agency networks."

The Government Accountability Office reports that the intrusion-detection capability has been implemented at 23 CFO Act agencies as of July 2015, but the capability has limited deployment at portions of five of these agencies.

Critics say that one drawback to the system is that it detects only known entities. For instance, at OPM, Einstein didn't initially pick up on a problem because it had not seen it before, Phyllis Schneck, Chief Cybersecurity Official at DHS, told the Wall Street Journal in June. But Johnson told CSIS that E3A is a platform for future technologies, including those that can automatically identify suspicious traffic even if the particular threat is unknown.

Einstein's Genesis

Each federal agency is responsible for its own cybersecurity, yet true protection requires a level of openness and sharing so that agencies can work together to address challenges and gain situational awareness — "the ability to identify, process and comprehend the critical elements of information related to an area of interest — in this case, cybersecurity."

To attain a common level of cybersecurity data collection, analysis and sharing, US-CERT developed Einstein. Data collection is passive, meaning it does not interfere with communications, and it meets mandated privacy requirements. **(See Page X for more on privacy.)**

According to the September 2004 Einstein Privacy Impact Assessment, the data collected under the program includes:

- **Autonomous System Numbers.** These identify a group of IP networks and let the group exchange information with other systems, or groups.
- **Internet Control Message Protocol Type/Code.** The protocol is used to communicate control messages between hosts and routers. Protocol packets can contain diagnostic, error, information or control messages, which are generally harmless, according to DHS, but not always.
- **Sensor identification and connection status.** This describes where a sensor is situated and whether it's receiving information.
- **Source and destination IP address.** This tells what device is sending data and where it should be going.

Legal Roots

Besides the need for better protections, several pieces of legislation were instrumental in Einstein's birth. The Federal Information Security Management Act (FISMA) of 2002 required the director of the OMB to oversee federal information security policies and practices, to coordinate a government-wide risk-based approach for managing such things and to run a federal information security incident center. That came in the form of the National Cyber Security Division's US-CERT.

Additionally, the Homeland Security Act of 2003 assigns DHS a major role in coordinating a government-wide cybersecurity approach.

At the end of 2014, FISMA was updated to authorize DHS to help OMB implement agency information and security practices. Under it, the department's secretary must develop and oversee the implementation of directives regarding the safeguarding of federal information. Johnson issued the first one May 21, requiring agencies to fix any vulnerabilities that NCCIC had identified on its networks. "Departments and agencies responded quickly, and have already reduced critical vulnerabilities covered by the Binding Operational Directive by more than 60 percent," Johnson told CSIS.

The new law also augments the scope of what kinds of information should be reported from primarily policies and financial information to specifics about threats, security incidents and compliance, according to National Law Review. What's more, the update requires that federal agencies provide notice to Congress no later than 30 days after they discover a breach.

Privacy Concerns

When data is involved, privacy concerns often are, too. Because Einstein collects and shares information, DHS must ensure that the system meets federal regulations for privacy protections. The department did this early on. Unsurprisingly given its name, the 2004 Privacy Impact Assessment addressed this issue at the outset.

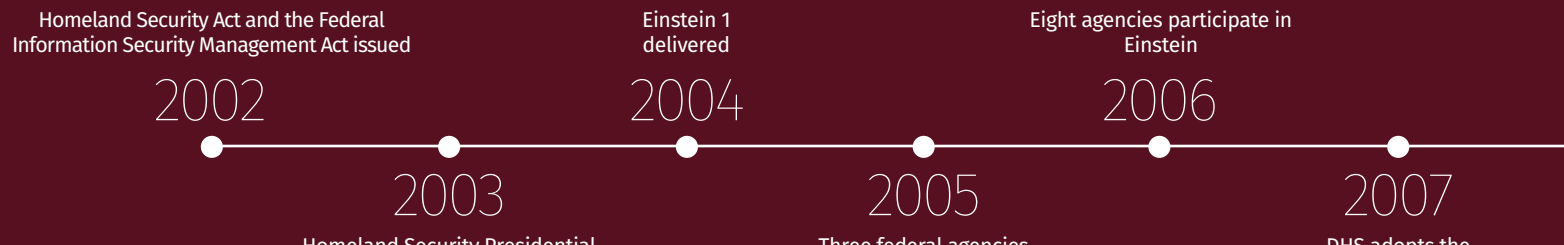
The rules that Einstein complies with, according to the assessment, are the Homeland Security Act, Homeland Security Presidential Directive 7 and FISMA. The system's process, it states, is as follows:

Einstein's Genesis

The U.S. Computer Emergency Readiness Team "has a responsibility to present a single, government-wide focus for monitoring and evaluating risk management and assessment activities based on identified government priorities, functions, and services," according to the 2004 Einstein Privacy Impact Assessment. It does this through the Einstein program.

The Federal Information Security Management Act (FISMA) of 2002 requires federal agencies to report on cybersecurity incidents

Einstein's Lifelong Timeline



First, Federal civilian agencies will collect subject data. Each agency will transmit to a secure US-CERT facility only that data that meet the criteria for anomaly detection and other IT risks. The US-CERT has structured the program to limit the amount of data collected.

Second, the US-CERT will then analyze data submissions. Analysts are trained to identify anomalous activity and will strictly focus only on such activities.

Third, where there are suspicious anomalies or other aberrations, the US-CERT analysts will collaborate with agency partners to examine more carefully additional network activity associated directly with such activities.

Fourth, in addition to providing information about potential anomalies and other aberrations, EINSTEIN will also be able to offer agencies counsel on configuration management options. The EINSTEIN Program will offer information and options based on a collective and collaborative approach.

Situational information generated as a result of EINSTEIN will also allow the US-CERT to generate a cross-governmental trends analysis. The analysis will provide departments and agencies with an accurate and aggregate picture of the health of the Federal.gov domain in real time, and an aggregate comparison of the health of the Federal.gov domain as compared to the Internet.

The document goes on to say that the information Einstein collects will be shared between US-CERT and participating federal agencies in increments. When anomalies are found, Einstein might ask for additional information as part of its investigation. The results of US-CERT's analysis are shared with the agency or possibly agencies and then it's up to them to act on the information, based on their own information-sharing policies.

When it comes to personally identifiable information, agencies must comply with notification and consent regulations, by, for instance, posting notices on their websites that computer security information is being collected. Agencies are also required to publish PIAs about PII that may be collected.

Any information transmitted to US-CERT via Einstein will be sent using a secured protocol, and access is limited on a need-to-know basis.

Where Einstein Stands Now

In September 2015, DHS awarded a $1 billion contract to maintain and improve Einstein as part of its five-year Development, Operations and Maintenance (DOMino) program. Little is known about DOMino because it came out of the department's classified portion of its acquisitions division, Federal News Radio reported, but it shows DHS's continued commitment to moving forward with the program.

"The DOMino contract will provide services to operate and maintain existing Einstein capabilities and will also be used to design and develop new cybersecurity capabilities for the NCPS," DHS spokesman S.Y. Lee told the Federal Times.

Another indicator of the department's support of cyber is its fiscal 2016 budget request for $1.4 billion, including $479.8 million earmarked for Einstein.

What's more, Sens. Ron Johnson (R-Wis.) and Tom Carper (D-Del.), the Homeland Security and Governmental Affairs Committee's chairman and ranking member, respectively, in July sponsored the Federal Cybersecurity Enhancement Act of 2015, which would mandate that all agencies adopt Einstein. The committee passed the bill and significant sections of the legislation were added as an amendment to the Cyber Information Sharing Act of 2014, according to Federal News Radio.

Also in July, Rep. Will Hurd (R-Texas) introduced the Einstein Act of 2015 to authorize DHS to deploy E3A. DHS Secretary Johnson has called on Congress to authorize the program's deployment.

The Homeland Security Act of 2003 gives the Homeland Security Department a major role in coordinating incident identification and reporting

DHS's National Cyber Security Division (NCSD) leads federal cybersecurity efforts

NCSD's operational arm is US-CERT, which is a partnership between the public and private sectors to compile and analyze security incident information, inform agencies about threats and vulnerabilities and consult with national security agencies and operators of national security systems.

Einstein is deployed at 15 of nearly 600 U.S. government agencies, departments and web resources.

2008

E3A deployed

2013

E3A protects 237,414 federal personnel

2014

Expected deployment of E3A

2016

2008

Einstein 2 delivered

2013

E3A protects more than 931,000 federal personnel, or about 45 percent of the federal civilian workforce

2015

DHS awards a $1 billion contract to maintain and improve Einstein

SPOTLIGHT:
Q&A with Ann Barron-DiCamillo,
US-CERT Director

DiCamillo has worked at DHS since 2012, initially leading NCCIC's Program Development and Capabilities Integration branch before becoming Director of US-CERT in January 2013. US-CERT, which has a round-the-clock operations center accepting, triaging and responding to incidents, was established in 2003 to protect the country's Internet infrastructure.

How has Einstein evolved?

Einstein is now officially 12 years old. The first iterations of Einstein capabilities were developed back in 2003. Einstein I, which is the first capability, provided net flow – network flow monitoring capabilities, which are designed to identify malicious cyber activity through changes and trends in the network traffic.

Fast forward five years [to] 2008 and DHS incorporated into those existing Einstein capabilities a follow-on version, with continued focus on network defense-in-depth with the introduction of Einstein 2 a network security intrusion-detection system, or IDS. Einstein 2 can help identify malicious or potentially harmful computer network activity in our federal executive agencies' network traffic based on specific signatures beyond those provided in network flow trends. Einstein evolved from just looking at the flow records into alerting on specific signatures of known malicious activity associated with the focused operations sets that are of importance to malicious activity directed at the government.

In 2010, DHS began planning for the design of an intrusion-prevention capability, and it was previously referred to as Einstein 3 to provide the government with an early warning capability, better situational awareness of intrusion threats to federal civilian executive branch networks and near real-time identification of malicious cyber activity while providing a better network defense. If you think about the defense-in-depth scenario of net flow and intrusion detection, intrusion prevention is the next natural step in network defense. In addition to detecting cyberthreats, this capability can block or disable attempted intrusions before any harm is actually done. If you're going to do blocking or disabling of network traffic, you must ensure it's known malicious cyber activity that is confirmed malicious.

In 2012, DHS transitioned the approach of the Einstein 3 program from building and deploying its own intrusion-prevention system to one in which DHS contracts with major Internet service providers to supply the intrusion-prevention security services. These services are augmented through the sharing of sensitive information or government information to those service providers, and this became known as the accelerated program, which is called Einstein 3 Accelerated, or E3A.

How do Einstein 1, 2 and 3 differ?

Einstein I is more analogous to a camera capturing license plate information. And just as a camera captures basic information about a passing car, Einstein I would detect characteristics of Internet traffic. We use this data within US-CERT to identify attempts at malicious activity such as distributed denial-of-service attacks as well as incident forensics, enabling us to look back in time and identify unusual changes in traffic patterns that could correspond to malicious activity. Just as law enforcement uses license plate camera data to determine whether malicious vehicles have passed a certain check point, we use net flow for incident response engagements, Netflow can be helpful in specifically identifying when there's potential data [exfiltration] that might have occurred. With net flow we can identify patterns of large volume of data that's outside the normal profile, which can be helpful for incident response teams to better pinpoint a timeframe. In that camera scenario, Einstein 2 is going to scan the car and send an alert to a security professional that a prohibited or potentially malicious vehicle has passed that checkpoint. Like a license plate camera system that is loaded with a list of known prohibited vehicles, Einstein 2 uses signatures of known malicious cyberthreats.

Continuing along with that analogy, E3A would be comparable to a guarded gatehouse at a highway checkpoint to multiple bases. In this analogy, the highway to multiple bases are the Internet service providers that serve multiple federal departments and agencies. Just as a gatehouse may access a sensitive list of prohibited vehicles, E3A uses classified information to block potential cyberattacks from impacting federal networks.

Is there a mandate to use Einstein?

Einstein's mandate is derived from a combination of statues and presidential directives, from FISMA Act of 2014, which authorizes in law DHS deployment of technologies to protect agency information and information systems. The Homeland Security Act of 2002 provides broad authority to DHS to access, receive and disseminate information regarding threats to homeland security including cybersecurity. HSPD 23/NSPD 54, which was passed in 2008, directs DHS to deploy intrusion-detection and prevention sensors across the federal civilian agencies. OMB memorandum M-08-05, Implemented the Trusted Internet Connections in 2007. This memo required all federal executive agencies to use Einstein 2 sensors.

Where does Einstein adoption stand now?

E1 and E2 sensors are currently deployed at 81 departments and agencies, which is roughly 85 to 90 percent coverage. As of October 2015, E3A services are deployed to about 23 federal departments and agencies, which covers roughly about 50 percent of the federal networks.

Is adoption happening fast enough?

Cybersecurity is a risk management area and, we can't eliminate all the risks. Agencies that implement best practices and share information will increase the cost for adversaries and stop many threats. Having the aspects of situational awareness the complement of Einstein systems provides across the dot-gov enables us to see the trends from one organization to another. One department's event can become another agency's prevention. We can insert an indicator of compromise (IOC) from one event into Einstein, to protect other government agencies and then share that IOC with other partners both domestically and internationally.

What's holding adoption back?

We expect coverage of federal departments and agencies to be complete by the end of fiscal year 2016.

U.S.-CERT and Einstein have taken heat after the OPM breach. How do you respond to that? What could have been done differently and what are you looking at changing now that the problem has come to light?

I think it comes back to what I said previously regarding cybersecurity is about risk management. You can't eliminate all risks. to drive up the cost for adversaries, but ultimately there's no perfect cyber defense and persistent adversaries who are well funded and have long-term horizons will find ways to infiltrate networks in both government and the private sector. The Federal Information Security Modernization Act of 2014 specifies that federal agencies are responsible for their own cybersecurity. As computer network defenders, we work in a shared partnership to help federal agencies improve their own cybersecurity. At US-CERT, we're actively assisting departments and agencies to protect their systems through sharing best practices, the Einstein program, our incident response efforts. We believe that continuing to build on the exemplary incident response team capable of assisting multiple customers simultaneously will augment the federal network security.

We're continuing to assist agencies by providing the latest in best practices, sharing threat information and trends through quarterly meetings, weekly analyst calls, monthly meetings at different levels, classified meetings with federal CIO and [chief information security officer] communities, and we're holding briefings on both multilateral engagements as well as bilateral engagements across the community. US-CERT is the hub for cyberthreat information sharing, and we stand ready to help assist federal departments and agencies and their security operations centers to increase their own capacities and capabilities.

> *"As network defender, I would want to leverage all the capabilities and tools that are offered to me as a network owner, especially the ones that are no cost to me as a department or agency."*
>
> *- Ann Barron-DiCamillo, US-CERT Director*

Following the OPM breach, OMB established a focused effort of the 30-day cybersecurity sprint to rapidly address some key cybersecurity deficiencies that had been identified across the government. DHS was a key partner in that effort. As an example, one focal point of the cybersecurity sprint called for agencies to identify and patch critical vulnerabilities for Internet-facing devices. These kinds of vulnerabilities are easily exploited and should be immediately fixed. No federal agency should have known vulnerabilities associated with Internet-facing devices. That's just a best practice, yet that was still not being addressed in a consistent manner across departments and agencies. The focus from the cybersecurity sprint helped align this directive from DHS Secretary Jeh Johnson, using the authorities DHS received in last year's FISMA legislation that called on agencies to fix these critical Internet-facing vulnerabilities within 30 days of the patch release. You want to give departments and agencies time to test these patches to make sure they're not breaking functionality, but we need to make sure that they're prioritizing the patching of critical vulnerabilities.

This is one of the efforts driven from events such as the OPM breach that helped move us forward in a positive way.... Based on this effort, agencies have patch almost all the critical vulnerabilities that we identified when this directive was issued..

Are there examples of Einstein success stories?

One of the important roles US-CERT plays is helping share information across agencies, and in cases, with the private sector. For example, as soon as OPM identified malicious activity on their network, they shared the information with US-CERT, and we deployed a signature for that particular threat. We used Einstein 2 to look for other compromises across the federal civilian government. This same threat information was used in E3A to also block potential threats to those federal networks. We used E3A to ensure that this cyberthreat could not be exploited at other agencies protected by the system.

What risks do agencies take by not adopting Einstein quickly?

Einstein provides continuous, automated monitoring and detection of malicious traffic, and can prevent that malicious traffic from harming the network. It's a broad, cross-cutting security capability that's available for all executive branch networks. As network defender, I would want to leverage all the capabilities and tools that are offered to me as a network owner, especially the ones that are no cost to me as a department or agency.

What are some best practices that agencies can use as they look at adopting Einstein?

Perimeter defense like Einstein is just one element of the defense-in-depth strategy to secure the federal executive branch networks. Einstein needs to be combined with other security measures such as network hardening, Continuous Diagnostics and Mitigation, application whitelisting, data segmentation, workforce security and training We're really foot stomping on the importance of data segmentation. Commonly, in incident response engagements we see a lack of data and network segmentation resulting in flat environments where it makes it really easy for adversaries to easily move laterally.

What are your goals for Einstein?

The goal of the Einstein set of capabilities is to provide [the] federal government with this early warning system and improved situational awareness of the intrusion threats to their infrastructure and networks. We want to provide near real-time identification and sharing of malicious cyber activities and ensure we're preventing identified malicious cyber activity from then trending across the dot gov.

THUNDERCAT TECHNOLOGY

riverbed®

A Service-Disabled, Veteran-Owned Small Business

Innovate, Grow, Know with ThunderCat & Riverbed.

WWW.THUNDERCATTECH.COM

Big Data & Analytics | Data Center Infrastructure | Enterprise Applications | Cyber Security

State of Cybersecurity

As you can see, CDM and Einstein are closely related, standing side-by-side in the fight against cyber threats. Rooted in the same legislation and ultimately serving the same goal of increasing protection and information sharing among federal civilian agencies, they both rely on commercial tools and services and are both part of DHS's National Cybersecurity Protection System.

So, it's not surprising that both are under similar scrutiny. After the OPM breach, critics raised questions about the effectiveness of CDM and Einstein. The breach happened when hackers – presumed to be from China – stole contractor login information. Einstein discovered the problem after being implemented at OPM in April, and a DHS spokesman told C4ISR&Networks that US-CERT cyber incident response teams were sent to identify the scope of the problem and help mitigate risks.

"US-CERT reviewed the malware and shared the analysis with the affected agencies and interagency partners, and deployed the signatures to Einstein to protect federal networks," according to C4ISR&Networks.

But that means "adversaries were inside the OPM network for 10 months before their malware signatures were plugged into Einstein," according to Federal Computer Week

Speaking before the House Committee on Oversight and Government Reform on June 16, Ozment told lawmakers that "as soon as OPM identified malicious activity on their network, they shared this information with DHS. DHS then developed a signature for the particular threat, and used Einstein 2 to look back in time for other compromises across the federal civilian government. This same threat information is used by Einstein 3A to block potential threats from impacting federal networks. Thus, DHS is using Einstein 3A to ensure that this cyber threat could not exploit other agencies protected by the system. DHS is accelerating Einstein 3A deployment across the federal government. While it is challenging to estimate the potential impact of a prevented event, each of these malicious (Domain Name System) requests or emails that were blocked by Einstein 3A may conceivably have led to a cybersecurity compromise of severe consequence."

Ozment pointed to the DHS National Cybersecurity and Communications Integration Center's successes, such as providing onsite incident response to 32 events in fiscal 2015, nearly double the total for fiscal 2014.

Of course, OPM is not the only government entity reeling from cyberattacks. A July GAO report lists others:

- The **Internal Revenue Service** said in June that hackers used taxpayer-specific data acquired from non-IRS sources to gain unauthorized access to information such as Social Security data, birth dates and street addresses on about 100,000 tax accounts.
- In April, the **Department of Veterans Affairs**' Office of Inspector General reported that two VA contractors had improperly accessed the VA network from foreign countries using personally owned equipment.
- In September 2014, a cyber intrusion into the **U.S. Postal Service**'s information systems may have compromised PII for more than 800,000 employees.

> *"Malicious actors aren't slowing down. As their efforts become more sophisticated, frequent and impactful, so must ours."*
>
> *- Tony Scott, Federal CIO*

Overall, faith in the government's cybersecurity is low. Only 6 percent of adults say they are very confident that government agencies can keep their records private and secure, and another 25 percent say they are somewhat confident, according to a survey Pew Research Center conducted in May – before the news about OPM came out.

In another survey last year, Pew found that 61 percent of respondents believed that a major cyberattack causing widespread harm would occur by 2025, while 39 percent said they didn't believe that would happen.

Government officials hope that programs such as CDM and Einstein can help restore some faith in their efforts to keep data safe. To emphasize their importance, federal CIO Scott was readying at the end of October 2015 a follow-up to the 30-day sprint held three months earlier that will likely push E3A and CDM.

"Agencies are reducing the number of privileged users and working with DHS to scan their networks on an ongoing basis for known critical vulnerabilities," Scott said in July. "Additionally, agencies continue to train employees to recognize and report phishing attempts to introduce malware into federal networks. But malicious actors aren't slowing down. As their efforts become more sophisticated, frequent and impactful, so must ours."

The Expanding Threat Surface

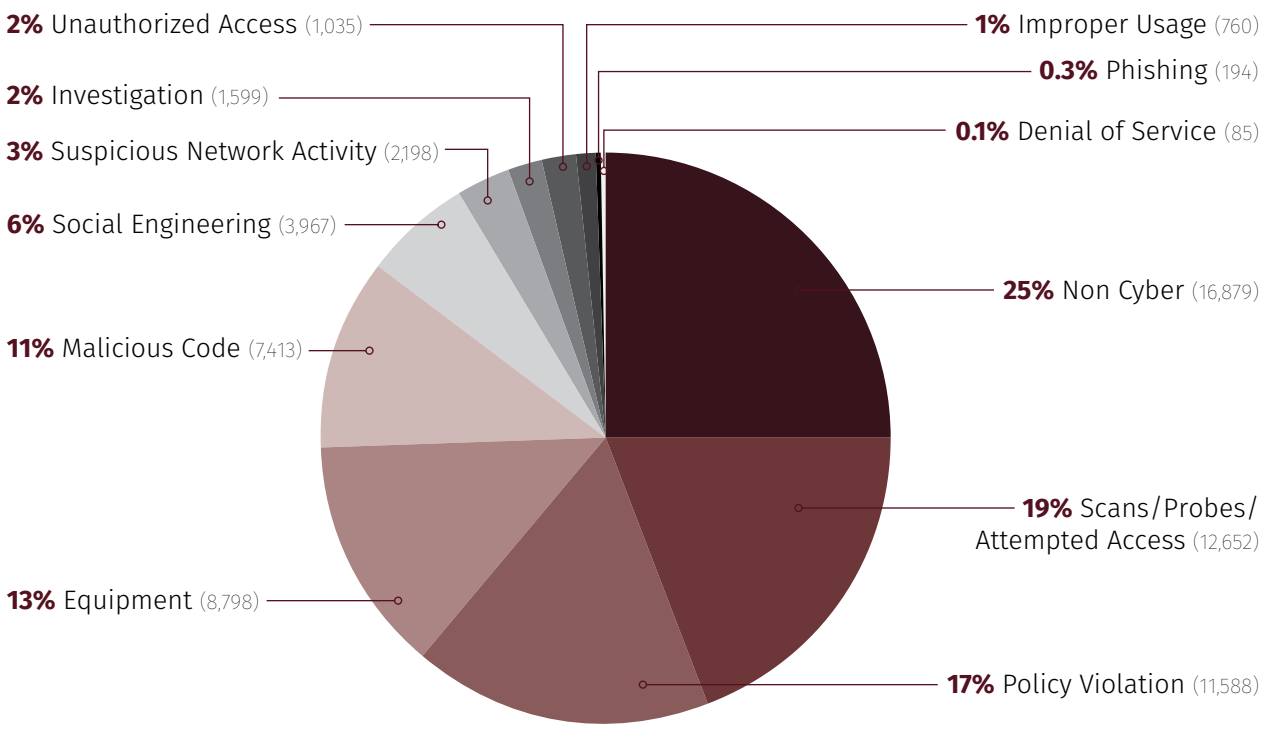
The fact is the threat surface — the points at which attackers could gain access to systems and/or data — is growing. As mobile devices proliferate and the Internet of Things emerges to connect ever more items to the web, cybersecurity is under constant stress to keep up. According to an August report by McAfee Labs, the number of security incidents in 2014 was 42.8 million, up from 9.4 million in 2010, and the number of connected devices has risen to 16.3 billion.

More specifically, federal cybersecurity incidents rose by 15 percent in fiscal 2014, according to the 2015 annual FISMA report to Congress. A July GAO report found that "the number of information security incidents affecting systems supporting the federal government has steadily increased each year: rising from 5,503 in fiscal year 2006 to 67,168 in fiscal year 2014, an increase of 1,121 percent.

"Furthermore, the number of reported security incidents involving PII at federal agencies has more than doubled in recent years — from 10,481 incidents in fiscal year 2009 to 27,624 incidents in fiscal year 2014," the report continues.

Still, it's not all doom and gloom: The FISMA report also states that 92 percent of agencies have continuous monitoring in place, up from 81 percent in fiscal 2013.

Information Security Incidents by Category, Fiscal Year 2014



Source: GAO analysis of United States Computer Emergency Readiness Team data for fiscal year 2014. | GAO-15-758T

Steps to Improving Cybersecurity

Experts emphasize that cybersecurity has no silver bullet and that cyber incidents are inevitable. Hackers have to be successful once; defenders have to be right all the time, and "those are impossible odds. No one can do that," said Isaac Porche III, Associate Director of the Rand Arroyo Center's Forces and Logistics Program and Rand Senior Engineer. "It's like being in a weak boat. Prepare for what happens when a hole comes in because you're going to have a hole at some point."

As a result, the focus seems to have shifted from prevention to incident response, but prevention continues to be a crucial part of any security strategy. That's where CDM and Einstein come in.

To combat the expanding threat surface, cyber experts recommend three steps, each of which the two programs can help with:

1. **Inventory** all applications and assets and then prioritize them.
2. **Address** insider threats by taking inventory of employees and minimizing the number with privileged access and increase use of multifactor authentication.
3. Don't set it and forget it. **Continue to monitor** for anomalies and known threats.

But these steps aren't as straightforward as they seem. Many agencies don't know how many computers are on their networks, Porche said. "The key phrase that comes up is 'Identify your key cyber terrain,' the key pieces of territory you have to defend, that you want to defend, because not everything you care about defending because it's just not that important," he said. "You can't put your resources into everything."

Monitoring is also problematic, he said, and needs to be more intelligent. "We do lots of monitoring now, but the state-of-the-art for monitoring is such that we get notices every day that something might be wrong, but they're false positives, and most network administrators will tell you, 'We get false positive messages in the thousands.' So, attackers hide in that," Porche said.

Another weak spot, wrote Richard Spires, Chairman of Resilient Network Systems and DHS CIO from August 2009 to May 2013, in a Federal Computer Week column, is that the Cross-Agency Priority Goals, which tackle common problems among myriad agencies, "typically consider objectives of less than 100 percent to be successful, such as 95 percent for automated asset management or 75 percent for strong authentication."

Mark Weatherford, Senior Adviser at the Chertoff Group and former Deputy Undersecretary for Cybersecurity at DHS, agrees that "good enough" is not enough. "People are still thinking vertically when they should be thinking horizontally," Weatherford said. "What I mean by that is we still think about security and our environments from a perspective of 'We have a perimeter and there's a logical progression of communications and data flow in that once you come through our environment,' when in fact the perimeter is gone."

Mobile technologies, cloud environments and virtualization have made vertical thinking distracting, he said. "We're still addressing siloed problems with siloed solutions, when in fact we have these very aggregated and enterprise problems that we aren't addressing," Weatherford said.

Spires recommends using enhanced automated protection so that IT administrators can use their time "detecting and remediating only the most sophisticated and potentially dangerous attacks rather than trying to decide which of the seemingly endless alerts to pursue today."

He also touts the protection of data, rather than the protection of systems. That way, the information is safe regardless of where it is.

"I have thought for a while is that really what we need to do is work much harder on protecting that information directly and swing our resources more to doing that and less to trying to protect all of our systems – the old perimeter concept," Spires said in an interview.

> *"We cannot treat security the way we treat everything else and the way we've done historically because this problem changes every single day. When you have static parameters, static rules, static guidelines, static laws, they're not flexible enough to be able to adjust as the threat changes."*
>
> *- Mark Weatherford, Senior Adviser, Chertoff Group*

But security is about more than technology. It's also about policy, strategy and governance. To that end, Weatherford proposes a complete overhaul of how the government approaches those things: "I think that we should be thinking about a consolidated security organization for the federal government. And by that I mean a single organization or maybe two organizations that share the infrastructure and the management of that infrastructure to secure all of the federal government."

As things are now, cybersecurity is too widely distributed to manage efficiently and effectively at the federal enterprise level, Weatherford said.

"We won't ever fully secure the entire federal government without some sort of I'm going to call it incentive, but that's probably too light of a term, but some sort of incentive that mandates and requires every federal agency to do certain things and then hold people accountable when they don't do that," he said.

In early October, the House passed a bill calling on DHS to set a formal cybersecurity strategy. It would mandate that the department act as "a cross-sector hub for federal and civilian cyber threat information sharing," according to The Hill. Another Johnson-Carper bill in the Senate, known as the FISMA Reform Act, would update the 13-year-old FISMA and give DHS authority to search for intruders on any government network without a formal request, according to The Hill.

Any cybersecurity legislation should contain three elements, Johnson told CSIS:

First, Congress should expressly authorize the Einstein program. This would eliminate any remaining legal obstacles to its deployment across the federal government. The House has passed H.R. 1731, which accomplishes this by ensuring agencies understand they are legally permitted to disclose network traffic to DHS for narrowly tailored purposes.

Second, we must incentivize the private sector to share cyber threat indicators with the federal government through the NCCIC in a manner that provides protection from civil and criminal liability for private entities that share threat indicators, and protects privacy.

Third, we need a national data-breach reporting system, in lieu of the existing patchwork of state laws on the subject, and enhanced criminal penalties for cybercrime.

The bill he's referring to, the National Cybersecurity Protection Advancement Act of 2015, would also expand NCCIC to enable it to use response teams to assist agencies and businesses. It also calls for a bigger role with state and local entities, making it a collaborator on cybersecurity risks and incidents and establishing a National Cybersecurity Preparedness Consortium to train state and local first responders and officials on cyberattack preparation and response.

Legislation could help, but it could also hinder, Weatherford said.

"I worry about legislation because legislation is static, and if I had one piece of advice for any large bureaucracy, it's that we cannot treat security the way we treat everything else and the way we've done historically because ... this problem changes every single day. When you have static parameters, static rules, static guidelines, static laws, they're not flexible enough to be able to adjust as the threat changes," he said.

Cloudera Enterprise

The big data cybersecurity analytics platform

cloudera.com/cybersecurity

cloudera

Industry Spotlight

CDM: Where Cybersecurity Meets Big Data

An interview with TJ Laher, Product Marketing Manager, & Sam Heywood, Director of Product Management, Cloudera

Continuous Diagnostics and Mitigation (CDM) requires constant monitoring to ensure government IT departments strengthen the security of their cyber networks. When the general public thinks of such monitoring, they generally think of enhanced personal identification systems, beefed up security perimeters, and network sensor capacity. What is often overlooked, however, are the technologies necessary to store, process, and analyze the petabytes worth of information needed for a comprehensive approach to CDM and cybersecurity at large.

One increasingly popular method to harness the volumes of information leveraged for cybersecurity is to deploy big data open source software (OSS) technologies. One of the most popular OSS technologies for big data is Apache Hadoop, a framework that allows for the distributed storage, processing, and analysis of large diverse data sets across clusters of industry standard servers.

TJ Laher, product marketing manager, and Sam Heywood, director of product management at Cloudera, an organization leading innovation in the big data OSS community, sat down with GovLoop to discuss how OSS and Cloudera can help agencies improve their cybersecurity postures.

How can agencies begin to leverage complex technology like Hadoop to improve their cybersecurity posture? That's where Cloudera comes in. Cloudera offers additional software to its core, open source Hadoop platform that takes the hassle out of deploying, managing, and securing the Hadoop environment so that agencies can focus on applying the technology to fight cyber crime. Cloudera calls this platform an enterprise data hub (EDH).

Cloudera's EDH allows agencies to manage massive volumes of multi-structured data at lower cost, making it the ideal platform to ingest data that can be applied to cybersecurity analytics. By leveraging Cloudera's EDH for improved cybersecurity and continuous monitoring, government agencies can:

- **Modernize cybersecurity infrastructure.** Organizations can implement and maintain a future-proofed platform for data growth that keeps up with current and forward-looking cybersecurity applications and use cases.
- **Achieve faster advanced threat detection.** Once an organization's information is on the platform, cybersecurity analysts can deploy behavior-driven advanced analytics and better visualize their information in order to decide which potential threats should be investigated.
- **Accelerate threat investigation and mitigation.** Upon determining which potential threats should be inspected and mitigated, analysts can do so faster and more thoroughly with access to full-fidelity data that spans multiple decades.

"Organizations usually struggle with determining where threats and breaches are because their data is not in one location," Heywood said. "They also lack sophisticated data analytics tools."

Cloudera's EDH can help government keep data in fewer siloes to better track and analyze potential cyber threats. One of the main differentiators of Cloudera from other OSS offerings is its ability to provide secure management of data, which is a necessity for government.

In other words, Cloudera's platform can enhance your organization's data management while simultaneously strengthening cybersecurity infrastructures. This helps government easily deploy and manage the complex OSS to improve data management and expand innovation, while keeping your data and agency safe.

"When organizations implement Cloudera's EDH into their core infrastructures they not only get to leverage leading open source technologies of today, but also future capabilities," Laher said. "We continue to evaluate open source projects in the community and fold them into our platform as customer needs dictate. This creates an ever-evolving, best of breed platform that leverages the innovation taking place in the expansive open source ecosystem."

The unification of CDM, cybersecurity, and big data has opened a world of possibilities for government. Cloudera is helping government agencies keep up with big data innovation while tackling their cybersecurity needs. Whether your agency needs a cost effective data management solution, advanced threat detection capabilities, or strengthened cybersecurity infrastructures, Hadoop-based EDH is the way of the future.

What's Next for Government Cybersecurity Beyond CDM & Einstein?

Staying ahead of cyberthreats is an immense challenge. As soon as the technology exists to combat one problem, another is born and new tools are needed.

In a Government Technology interview in September, Ozment said he sees three key changes coming to cyber defense: "First, we must continue our progress in developing post-signature defense that relies on mathematical analysis of potential threats. Second, we must focus on the implications of a broad transition to cloud and mobile technologies. And third, we must move away from stove-piped cybersecurity tools and apply data analytics to help us holistically understand and manage cybersecurity threats."

To the first point, DHS is "developing advanced malware and behavioral analysis capabilities that will automatically identify and separate suspicious traffic for inspection, even if the precise indictor has not been seen before," he told GovTech.

Additionally, the department has partnered with GSA to develop guidance on securing cloud solutions.

"As the result of this effort, cloud service providers (CSPs) are beginning to provide innovative tools for their government customers to gain situational awareness of the security in the cloud," he told GovTech.

Lastly, Ozment said, DHS will rely on data to identify new threats and will share that information using a common schema called Structured Threat Information eXpression/ Trusted Automated eXchange of Indicator Information. STIX is a structured language for cyber threat intelligence, while TAXII defines a set of services and message exchanges that enable cyber threat information sharing.

A third information-sharing effort at US-CERT is Cyber Observable eXpression, which the agency defines as "a standardized schema for the specification, capture, characterization and communication of events or stateful properties that are observable in all system and network operations."

DHS Secretary Johnson also pushed the importance of information sharing to the future of federal cybersecurity in his talk at CSIS: "In order to sufficiently address the rapidly evolving threats to our cyber systems, we must be able to share cyber information as quickly, in as close to real time, as possible."

He highlighted the department's support of the development of Information Sharing and Analysis Organizations, which will link government and private-sector organizations. Also to that end, Johnson said DHS has its own system to automate the sharing of cyber threat indicators, but he wants to extend that capability government-wide. Additionally, DHS is working to establish the Cyber Threat Intelligence Integration Center, which "will help us better understand the various threats and provide more actionable and timely intelligence to the NCCIC to share with our private-sector partners."

The government is also stepping up its response to cyber attacks in an attempt to make the punishment not worth the crime. In January, Obama proposed changes to prosecution for various cyber offenses, including fraud and money laundering. The Defense Department's new Cyber Strategy addressed deterrence, too. Michael Rogers, Commander of U.S. Cyber Command, told the Woodrow Wilson International Center for Scholars in September that the United States must lead opponents to believe cybersecurity is so strong they will fail, but should a breach occur, it wouldn't bring them much value.

"It's part of the reason that when we came up with the [DoD cyber] strategy — in an attempt to deter behavior — we would talk about the department's intent to generate a spectrum of capability from the defensive to the offensive," Rogers said.

Indeed, on Oct. 16, the Justice Department charged a hacker in Malaysia with stealing U.S. service members' personal data and passing it to ISIS, according to the Washington Post. The charges are the first against a suspect for terrorism and hacking, according to the Post.

Q&A With Mark Weatherford,

Former Deputy Undersecretary for Cybersecurity at DHS

Mark Weatherford was Homeland Security's first Deputy Undersecretary for Cybersecurity when he served between 2011 and 2013. Now a Senior Adviser at the Chertoff Group, co-founded by former DHS Secretary Michael Chertoff, Weatherford offers a look at the federal government's approach to cybersecurity from both an insider's and outsider's point of view. GovLoop spoke with him about his take.

Einstein 1 came out in 2004, then 2 in 2008. And now it's almost eight years later and we are just seeing Einstein 3A emerge. Why the long delays?

Certainly there are new technical challenges to each new phase of it because they are significantly different, but there's also a significant amount of bureaucracy involved, and 3A is actually being used now, but the bureaucracy has been working with the Internet service providers that provide Internet services to the government. A significant amount of the work from 3A is going to be in the hands of the Internet service providers.

Do you think the Continuous Diagnostics and Mitigation and Einstein programs are moving forward quickly enough?

Nothing is moving forward quickly enough. Einstein is not moving forward quickly enough, but I would say that's a problem that everyone in private industry and government is having with getting products out there that can identify and mitigate the threat. The threat is just expanding far faster than most technologies are able to keep up with.

Both systems are under fire after the OPM hacks. Do you agree with the critics that the systems didn't do enough?

Security is like a Swiss Army knife. There are a whole lot of different things and not one tool is appropriate for every threat, so there are multiple tools out there that need to be deployed, some of them working individually, some of them working with other tools to provide the appropriate level of threat and vulnerability mitigation. … The tools were not deployed appropriately, which is how the OPM event happened.

What are some challenges with CDM and Einstein going forward and how can they be addressed?

There are 17 prime contractors for CDM and each of these prime contractors was selected by [the General Services Administration] based on the technology suites that they selected to be part of their portfolio of CDM tools and services. Well, they were selected and it's a fairly static selection. You have what you have. The problem is that technology is changing every day. There are new products coming out, new companies popping up, so for a new technology and a new company that comes alive today and has the best new thing that could fix some of that stuff, now they have to figure out how they can go and get on one of these prime contracts as a preferred vendor. That's an incredible challenge for them to do that. Part of the problem is you have a static list of tools and services in a very dynamic world.

What does the future look like for these programs in your ideal world?

I think there are tools in the private sector that will do almost everything that Einstein does at a far, far lower cost, and the value of that is obviously in the cost, but also private industry is incentivized to be flexible and adjust and adapt on a very, very rapid basis, so as the threat model changes as new vulnerabilities come up, the private sector is able to adjust to those – develop new products, develop new patches – whereas Einstein, while it will be able to adapt, it's a different incentive model when you have one customer – i.e., the government – verses as a private company when you have millions of customers.

In my perfect world, the government would take the requirements for Einstein and they would let the private sector solve that problem.

CDM, the challenge there is in the acquisition process, as I said … CDM was built around private-sector tools, but I know companies right now saying, "I have a good tool to add into the continuous monitoring stack of tools, but I can't figure out how to get on one of the prime contracts with one of the prime contractors." What that means is you have great products sitting out there languishing.

Conclusion

When it comes to cybersecurity, a lot of factors are in play. It's not just about technology, but also policy, legislation and process. All of those elements need to be fluid at a time when the threat landscape is growing by the moment. To get and stay secure, the government must be as agile as possible. That means creating and procuring state-of-the-art technology and deploying it enterprise-wide without delay.

DHS, which is tasked with handling cybersecurity for federal civilian departments and agencies, is working hard to stay on top of emerging problems while also playing catch-up in terms of technology deployment. It's got many subsections – US-CERT, NCCIC and CS&C make up a spoonful of the alphabet soup – committed to cyber resources. And leaders continue to look for more ways to improve those divisions' effectiveness.

"To be frank, our federal cybersecurity is not where it needs to be. But we have taken, and are taking, accelerated and aggressive action to get there," DHS Secretary Johnson said.

CDM and Einstein may not be perfect, but experts agree that no single cyber defense is. They are, however, crucial weapons in the federal government's cyber arsenal. And as subsequent phases and iterations of each roll out, the capabilities of each will continue to grow, offering the government better means to detect, prevent, mitigate and respond to cyberattacks.

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 200,000 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 info@govloop.com.

1152 15th St NW, Suite 800
Washington, DC 20005

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

www.govloop.com
@GovLoop

Acknowledgments

Thank you to Cloudera, HP, Merlin International, Riverbed and Thundercat Technology for their support of this valuable resource for public-sector professionals.

Author:

Stephanie Kanowitz

Designers:

Jeff Ribeira, Creative Manager
Tommy Bowen, Graphic Designer
Kaitlyn Baker, Junior Designer
Martin Nera, Design Fellow

1152 15th St NW, Suite 800
Washington, DC 20005

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

www.govloop.com
@GovLoop