CYBER SECURITY
EXCHANGE
MeriTalk

CDM
UNDER THE HOOD

GENERAL DYNAMICS
Information Technology

hp

IBM

RSA

REDSEAL
NETWORKS

Symantec

tripwire
CONFIDENCE: SECURED

Getting Under the Hood

Continuous Diagnostics and Mitigation (CDM) is starting to become a reality as an Information Systems Continuous Monitoring (ISCM) approach for civilian agencies across government. The Department of Homeland Security (DHS) is leveraging a Congressional appropriation to purchase critical cyber security products, including tools and sensors, that enhance and expand department and agency ISCM capabilities.

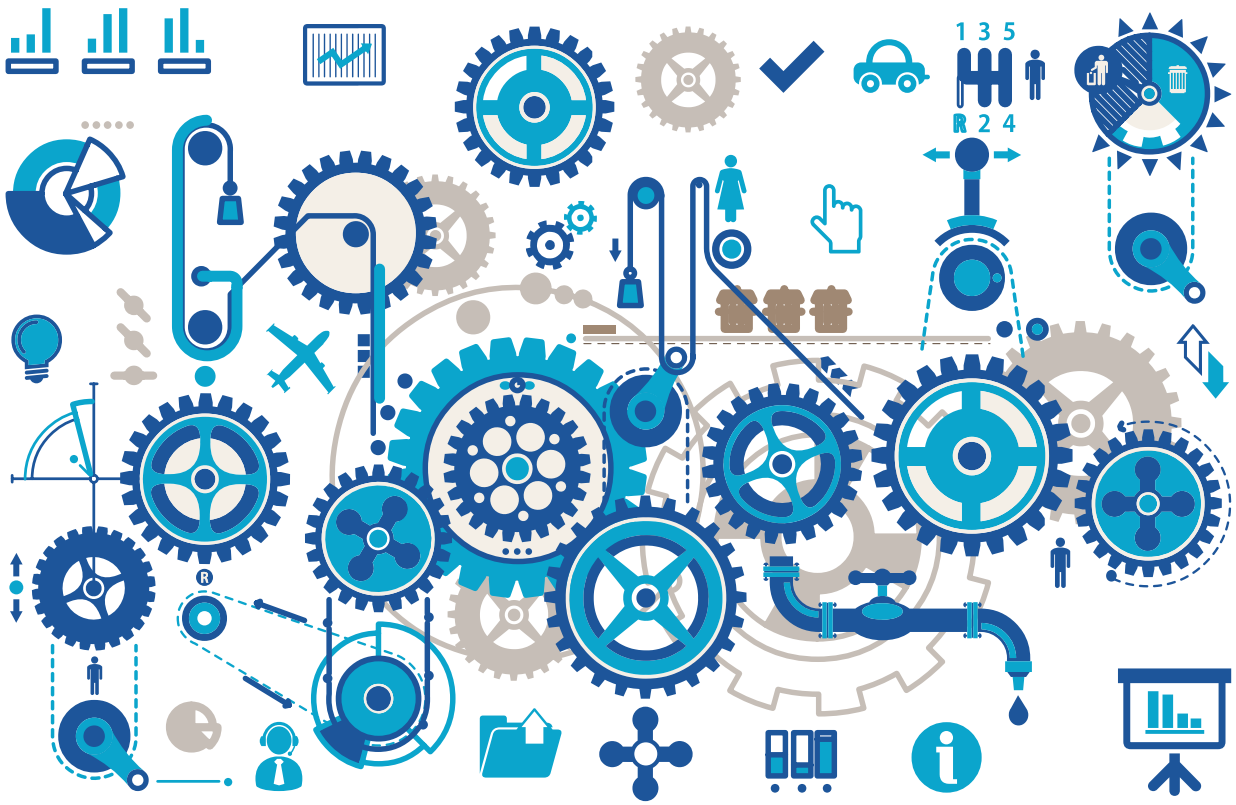
The CDM Task Order 1 is already providing nearly $60 million worth of CDM tools and sensors. Released in mid-March 2014, CDM Task Order 2 is focused on the implementation of a Federal-level cyber security dashboard. This latest task order award was the second in what is expected to be a series of contracts under the $6 billion CDM program.

So where are we? OMB required all agencies to develop CDM/ISCM strategies by February 28, 2014. Further, agencies must finalize their CDM/ISCM implementation plans and meet initial purchasing requirements by the end of FY 2014. MeriTalk interviewed 152 Federal cyber security/CDM leaders to get under the hood and reveal progress to date.

On the other side of the road, industry partners play a critical role in the successful roll out of CDM – providing the tools, experience, and knowledge. The success of the program lies within these public-private partnerships – providing vital products, solutions, and the capabilities of CDM tools to identify vulnerabilities and help protect the data and networks in today's 21st century cyber environment.

This report takes a look under the hood into who's doing what, progress made, and understanding challenges to date. It also provides the industry – CDM partners' – points of view. MeriTalk brings these partners together to shed light on progress and identify what is needed to ensure its success.

– Steve O'Keeffe, Founder, MeriTalk



Service Report

Since the CDM BPA was awarded in August 2013, many agencies are well on their way to planning for and adopting CDM:

- DHS reports that 96.7% have met the April 30th deadline to identify ISCM managers and resource/skills gaps that need to be filled
- DHS reports 87.8% have met the May 30th deadline to deploy products to support ISCM and be in accordance with Federal requirements

Despite progress, security managers are anxious to pick up the pace:

- 58% say the CDM program phases are rolling out too slowly, and 51% say the task orders are not being processed fast enough to support deployment of Phase 1 solutions
- Additionally, CDM goals require assessment cycles to fall under 72 hours, but 90% of security managers say information should be refreshed within one day

Managers are excited about CDM for good reason:

- Security managers praise CDM for a variety of benefits, including risk assessment and mitigation opportunities
- Many also believe CDM will improve decision making, including 53% who believe CDM will improve the overall culture of risk management in government

How do we get there from here?

- Security managers say the biggest barrier to CDM implementation is training IT and security staff; to optimize rollout managers need greater collaboration and IT automation
- To optimize CDM rollout, agencies call for cross-agency collaboration, more specific guidance, and greater analytical capabilities

Off and Running

According to DHS, many agencies are well on their way to planning for and adopting CDM*

Deadline Check-In

April 30th Deadline

96.7%

of individuals have identified specific individuals to manage the agency ISCM program and identified resource/skills gaps

May 30th Deadline

87.8%

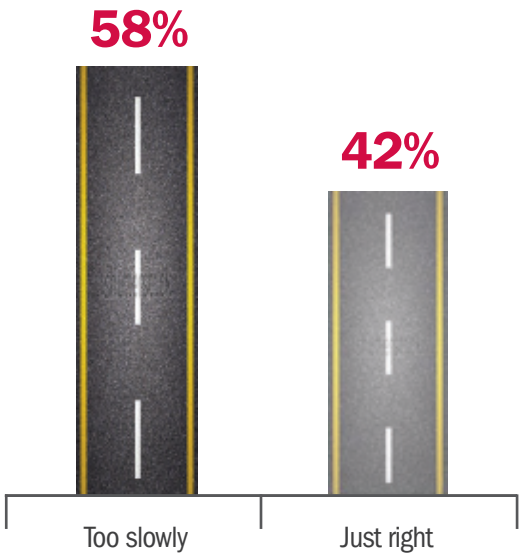
of agencies have begun to deploy products to support ISCM of all systems and are operating in accordance with Federal requirements

*As reported by DHS in March 2014

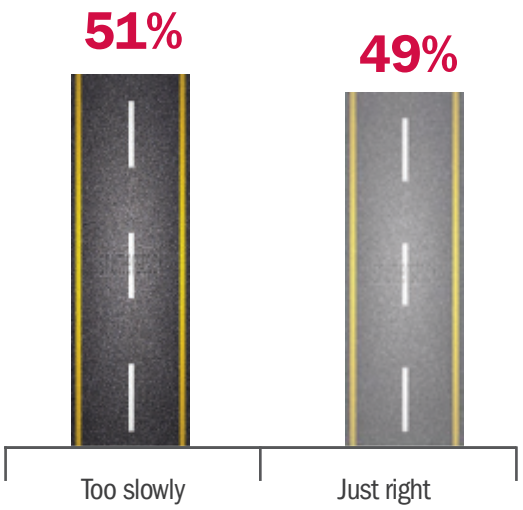
Pick Up the Pace

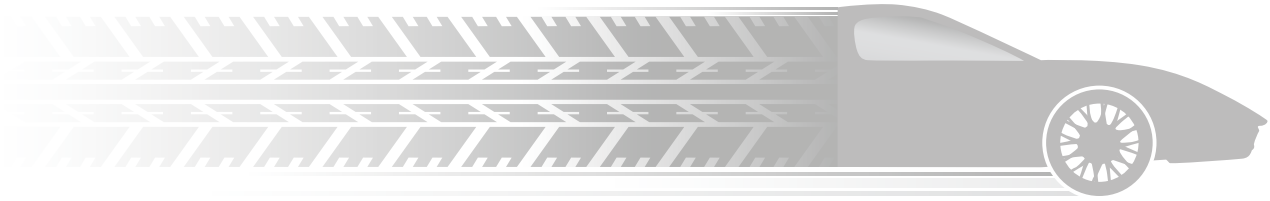
Despite progress, security managers say the CDM roll out is not fast enough

In your opinion, are the CDM program phases rolling out in a timely manner?



In your opinion, are the task orders being processed in a timely fashion to support deployment of Phase 1 solutions?





Quicker Lap Time

CDM goals require assessment cycles to fall under 72 hours, but 90% of security managers want information to be refreshed everyday

In your opinion, how often should assessment and discovery information be refreshed?

As real time as possible **32%**

5-10 minutes **7%**

30-60 minutes **17%**

56% within one hour

6 hours **13%**

12 hours **5%**

24 hours **16%**

90% within one day

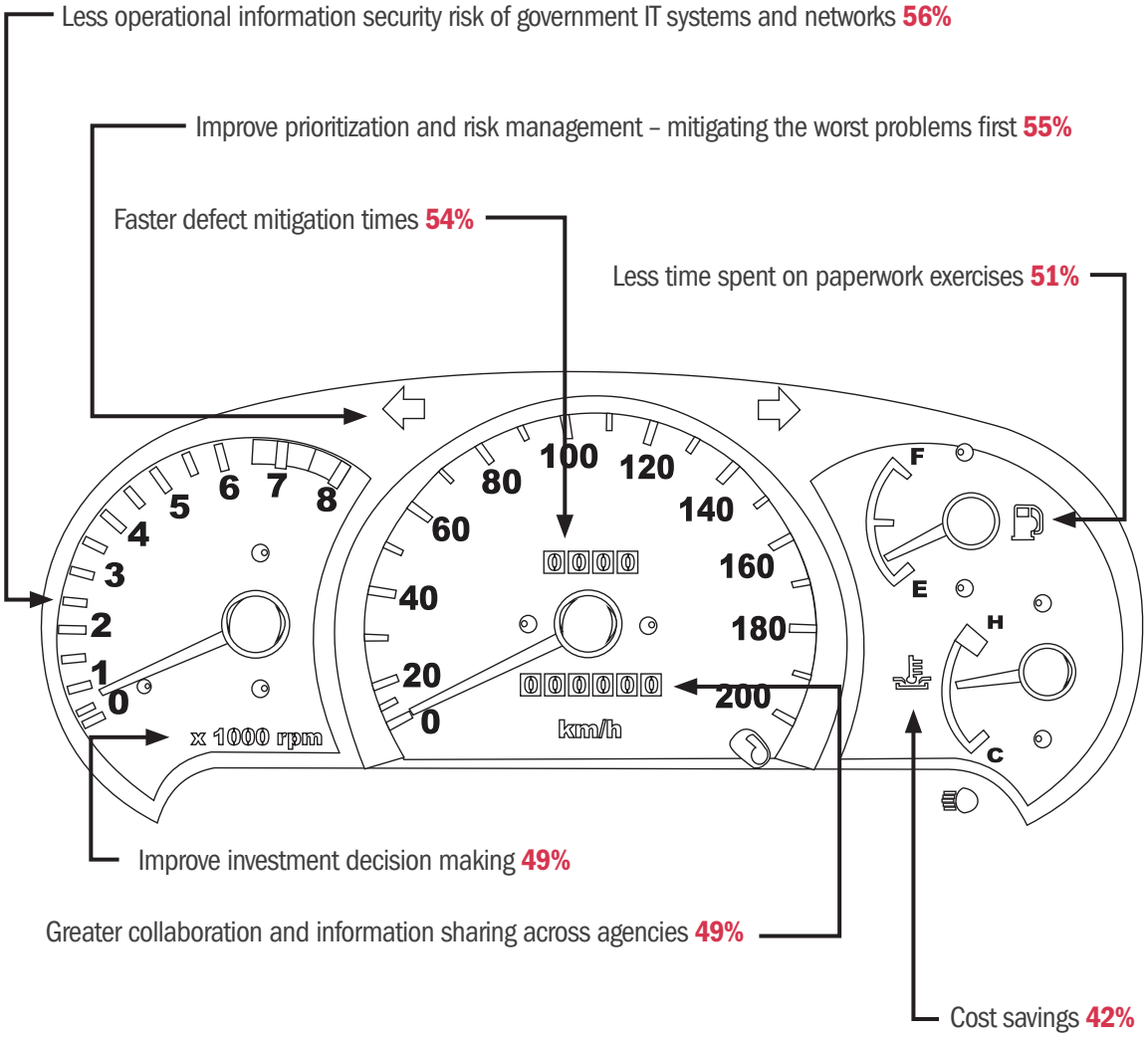
72 hours **5%**

96 hours or more **5%**

Owner's Manual

Security managers praise CDM for a variety of benefits, including risk assessment and mitigation opportunities

What are the benefits to implementing CDM/ISCM in your agency?*



*Respondents asked to please select all that apply

Signaling for a Turn

Many also believe CDM will improve decision making, including 53% who believe CDM will improve the overall culture of risk management

How will CDM affect decision making?*

- ✓ Improve risk assessment and acceptance **53%**
- ✓ Assist in deciding when to share data with other networks **50%**
- ✓ Improve awareness of consequences resulting from the current state of security **50%**
- ✓ Improve culture and collaboration **47%**
- ✓ Improve staff performance assessment **42%**
- ✓ Improve investment decisions **36%**

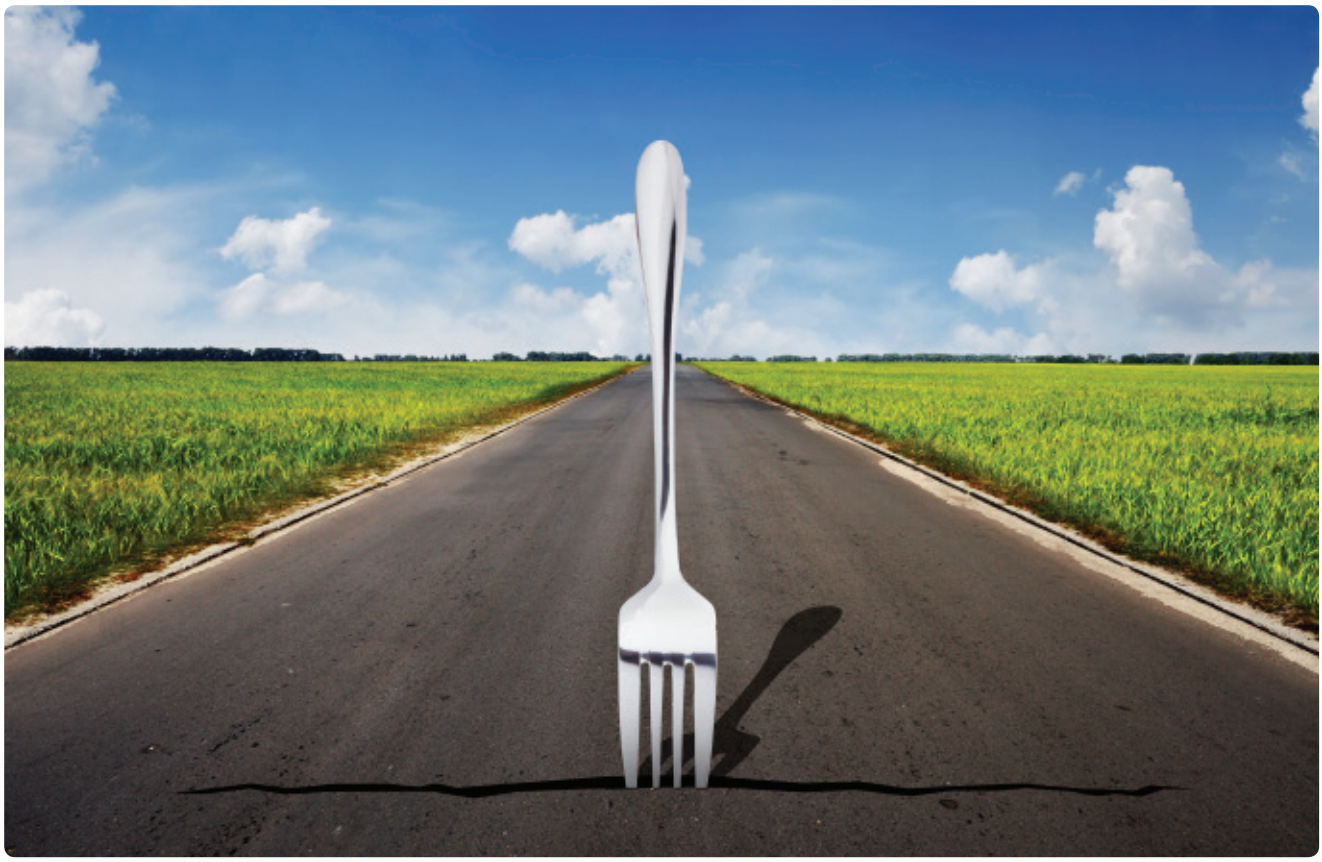
*Respondents asked to please select all that apply

Fork in the Road

CDM will not change FISMA overnight

In your opinion, with the shift to CDM/ISCM, is there a need for the current FISMA reporting requirements?

- Yes, because the CDM/ISCM program will not produce the data to replace the current system **20%**
- Yes, until the CDM/ISCM program produces enough data to replace the current system **50%**
- No, we have enough data now to replace the current system **13%**
- Unsure **17%**



*Respondents asked to please select all that apply

Crash Test

Agencies see opportunities for efficiency in automation

What are your future plans for managing FISMA reporting requirements?*

- Automation of monthly reporting **36%**
- Substitution of automated dashboard for much/all current annual reporting **26%**
- No change **24%**
- Substitution of automated dashboard for much/all current quarterly reporting **16%**

*Respondents asked to please select all that apply

FISMA Per Gallon

Managers spend a quarter of their wallet on gas

Respondent's spend approximately one quarter (25%) of their IT security budget on FISMA compliance.

Turbo Charge?

To successfully implement CDM, agencies' request greater analytical capabilities above all

What do you need to successfully implement CDM?*

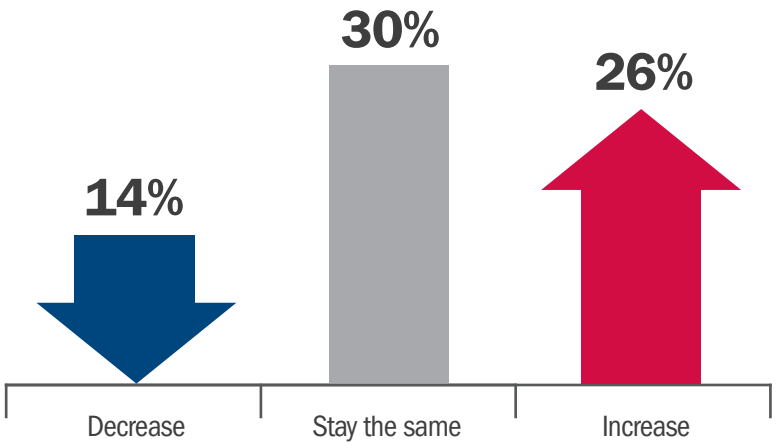
- Greater analytical capabilities **59%**
- Critical application resilience **57%**
- Common trusted identities **56%**
- Secure shared service environment **56%**
- More automated tools **55%**
- ROI and metrics **50%**
- More buy-in from the cyber workforce **48%**

*Respondents asked to please select all that apply

Leak in the Tank

Managers do not expect CDM to decrease FISMA spending

How will your FISMA-compliance budget change because of the focus on CDM implementation?*



Top Gear

Security managers ask for additional training, budget, and technical assistance for CDM success

What are the largest barriers to CDM?*

- Training IT and security staff **56%**
- Budget **55%**
- Difficulty integrating legacy systems **53%**
- Technical complexity **52%**
- Culture **51%**
- Complexity of/requirements for the CDM acquisition **49%**
- Acquisition process **44%**
- Lack of leadership support **40%**

*Respondents asked to rate on a scale from 1-5, where 1 is not a barrier and 5 a significant barrier

Pedal to the Metal

Security managers don't want to work alone – they seek consultation with other agencies and concrete CDM strategies and guidance

What additional guidance would be helpful to better develop your CDM strategy?*

1. Consultation with an agency that has completed a CDM strategy **36%**
2. Better documentation of Federal ISCM strategies **34%**
3. Concrete guidance and training on implementation of tools **33%**
4. More specific standards and guidelines **31%**
5. An example of an approved ISCM strategy **30%**

DHS reports additional toolkits and training available at: www.us-cert.gov

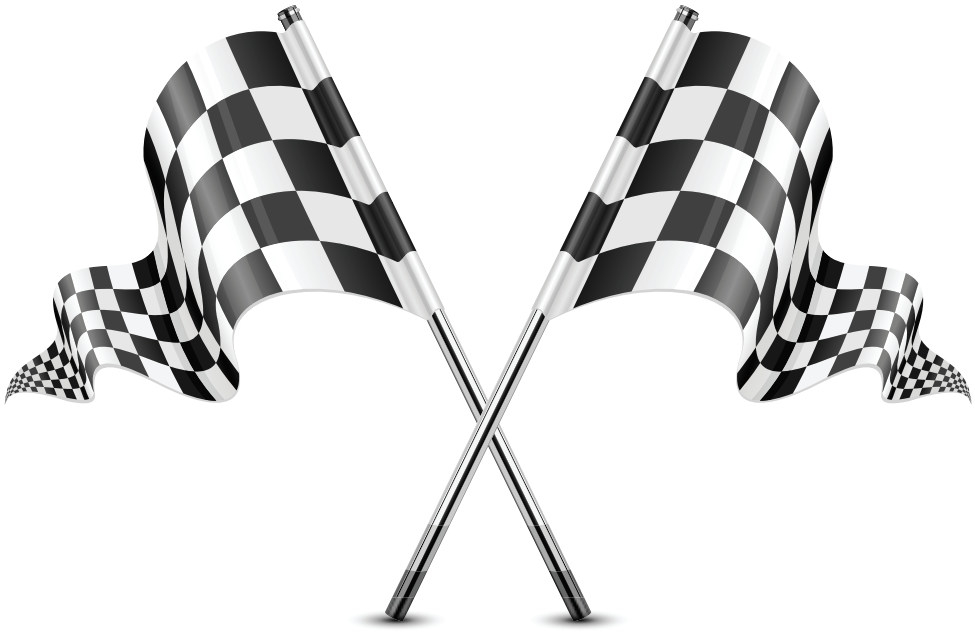
*Respondents asked to please select all that apply

Checkered Flag

Those working with CDM today believe that proper planning and cross-agency collaboration are critical to success

What is the most important lesson you've learned from the CDM/ISCM process to date?

- ✓ "Review all guidelines and procedures early and thoroughly before beginning implementation plan"
- ✓ "Be open to other solutions than those currently running"
- ✓ "Get all IT personnel onboard, including senior IT leadership"
- ✓ "Collaborate on lessons learned from other Fed agencies of similar size and function"
- ✓ "Project planning, management, and executive buy-in are crucial to successful implementation"
- ✓ "Flexibility is the key to success"



*Respondents asked to please select all that apply

Methodology and Demographics

MeriTalk conducted an online survey of 152 cyber security professionals responsible for the CDM initiative in May 2014. The report has a margin of error of ± 7.92% at a 95% confidence level.

Job Title:	
8%	CIO/CTO/CISO
14%	Deputy CIO/CTO/CISO
11%	Cyber Security Director
20%	Cyber Security Manager
47%	Cyber Security/IT Specialist/Manager

Agency Type:	
41%	Fed. Civilian Dept.
12%	Federal Civilian Component or Agency of a Department
8%	Federal Civilian not part of Department
39%	DoD or Intel

*Respondents asked to please select all that apply

CYBER SECURITY
EXCHANGE
MeriTalk

In conjunction with this study, the MeriTalk Cyber Security Exchange interviewed industry CDM partners providing tools and services on the BPA contract.

How can vendors help the success of the CDM program with government agencies? What is their perspective on the programs thus far? Turn the page to find out.

GENERAL DYNAMICS
Information Technology

hp

IBM

RSA

REDSEAL
NETWORKS

Symantec

tripwire
CONFIDENCE: SECURED

General Dynamics Information Technology – A History of Cyber Success

At General Dynamics IT, CDM/Continuous Monitoring as a Service (CMaaS) is their business. The company has been engaged with DHS since the agency began developing the parameters of the landmark CDM/CMaaS program, offering valuable and unique guidance.

Deeper Insight

This real world, mission critical experience has helped General Dynamics develop a Continuous Monitoring solution that is likely to be viewed as the most comprehensive available. The company is focused on hardening networks for clients, including .gov networks, in real time with its turn-key network monitoring and security-risk mitigation tools and services. Because of their time-proven solutions, General Dynamics knows the external risks unique to government computer networks and the increasing pressure government agencies are under to harden their networks with solutions that fit them best and fix their worst problems first.

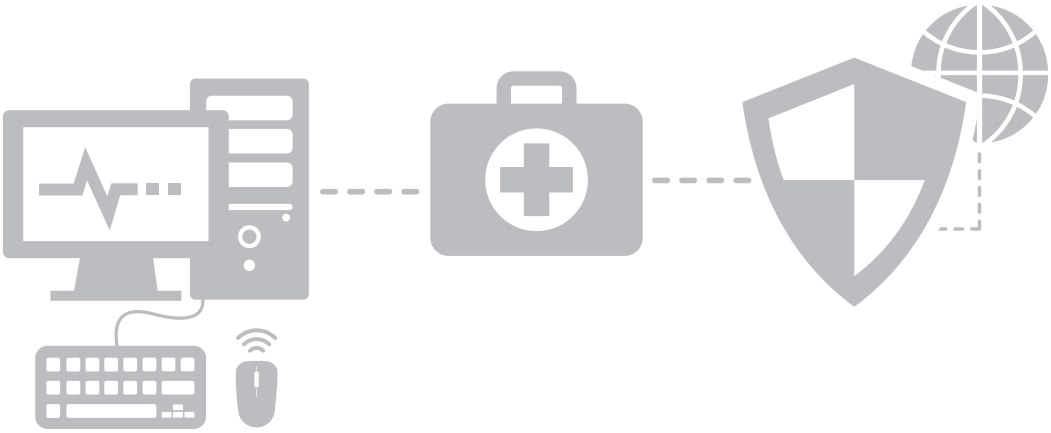
The company also understands that some agencies require a higher level of support than others, and General Dynamics have positioned themselves to provide the solution and to offer the guidance necessary to boost cyber security. From a truly plug-and-play framework, to customized cyber security capabilities, to full Project Management Support, to Training and Governance in CDM, General Dynamics intends to be a total solutions partner.

Range of Options

The first phase of CDM focuses on hardware and software asset management, configuration settings, known vulnerabilities, and antivirus. Those are the most fundamental areas of focus necessary to protect data. General Dynamics' capabilities are established at every level of the network, not just a network's periphery, giving agencies the ability to see how effective their systems are. In fact, the scope of General Dynamics' monitoring solution is repeatable and so vast that nearly every agency will find it easy to implement and use, and sure to fulfill any outstanding security need.

General Dynamics has been assisting agencies understanding how to order under the CDM vehicle to meet specific monitoring needs and can install, configure, and maintain dashboards; operate data feeds to and from dashboards; install, configure, and operate a wide range of tools, sensors, and custom-made sensors; integrate and maintain interoperability between a range of existing and new CDM tools; and support independent verification and validation efforts and system certification.

General Dynamics has the cyber capabilities and unique experience to meet the security challenges of today and tomorrow.



Wasif Shakeel
Senior Director for Continuous Monitoring and Diagnostics and Cyber Security Services
Health and Civilian Solutions Division

HP Enterprise Services – A Game Changer

It's important to know your turf.

HP is no stranger to the Federal government landscape. And it's no stranger to cyber security. Both are on HP's turf, where its been in the game for more than 40 years providing security innovation and monitoring expertise to Federal clients.

A Broader View

HP's Continuous Monitoring solution is notable for both the breadth and depth of its approach to tackling problems posed by the increasing complexity and volume of cyber threats.

Agencies require total situational awareness. HP Continuous Monitoring provides the analysis, design, installation, operation, and maintenance of diagnostic tools agencies need to operate in the current threat environment; see real-time threats and vulnerabilities; and measure risk.

HP tests, evaluates, and integrates a variety of security products for its customers - tailoring the best solution for a specific customer's environment. Its architecture is open and flexible, and as such, HP selects the right toolsets based upon the customer's needs.

Once deployed on a network, the tools recommended by HP perform the hardware asset management, software asset management, configuration management, and vulnerability management that serve as the foundation for all other Continuous Monitoring capabilities. With those pieces in place, agencies can more easily implement additional capabilities such as identity management and network access controls.

Greater Than the Sum of its Parts

HP sensors and dashboards give IT professionals the ability to visualize real-time malicious activity throughout a network. Armed with time-sensitive information, IT professionals are able to identify an immediate course of action, quickly mitigating the risks posed by cyber threats. Knowing your risk is one thing; but having the ability to respond immediately and appropriately to a security threat is equally vital.

Taking Note

Others throughout the industry have taken notice of the value of HP's cyber security solutions. Specifically, Gartner has recognized HP as a market leader in cyber security products and services due to its extensive experience with designing, implementing, and integrating complex technology solutions for both public and private sector entities.

HP has already delivered Continuous Monitoring solutions for multiple agencies, resulting in meaningful outcomes to CISOs and mission support personnel. HP's success with implementing Continuous Monitoring, combined with its open and flexible architecture, affords customers a best-in-breed solution to help secure systems from the core.

Additionally, HP also invests significant resources into the ongoing research and development of new and innovative technology solutions and conducts extensive product testing and integration in its labs prior to deployment. This helps ensure that its solutions, including continuous monitoring, will work in any environment, can be implemented quickly, with less risk, and at lower cost. This investment gives HP the advantage of knowing which solutions work best within a particular environment before an engagement begins so there is no "learning on the job."

Agencies have to be in the game. They can gamble on a newcomer or put their trust in a company that knows its turf.

Ed Keegan
Director, Cybersecurity
Solutions Group Portfolio

Gregg Hawrylko
CDM/CMaaS BPA
Program Manager

IBM – Seeing the Whole Picture, Frame by Frame

IBM has a broad view of the cyber security world. The company monitors 15 billion security events per day for public and private sector clients in more than 130 countries.

But IBM doesn't only focus on the big picture.

The company understands that no agencies in the Federal government are the same and each has its own unique needs. Agencies use networks differently. Their data is different – and valued differently. And their risks are different.

One big picture gleaned from many distinct perspectives.

In Focus

IBM, the world's largest information technology company, has built its CDM capabilities around DHS's three pillars – tools, service, and governance. Its mantra of flexibility allows agencies to pick and choose any component of its solutions to ensure security and compliance.

IBM provides one of the largest sets of CDM capabilities, with industry leading software solutions in the areas of endpoint management and compliance, application and database security, and security intelligence.

Like IBM itself, the IBM CDM solutions focus both on the broad picture while also bringing the granular view into focus. Endpoint management sees what's occurring on each device – no matter what device an employee uses – and ensures that the device remains in compliance. Security intelligence sees what's happening with the network, unifying data so agencies can see many events through a single lens.

Since IBM integrates its security intelligence capabilities with other solutions, it aggregates and then analyzes data from more than 400 pre-defined monitoring tools.

CDM A La Carte

IBM capabilities for endpoint management and security intelligence are effective no matter what architecture agencies have in place, which is significant because of the wide IT variety that agencies have developed to support their missions. IBM's solutions also allow agencies to order from the cyber security menu a la carte – taking as much or as little as they need to support their cyber security efforts.

The solutions also are known for being easy to deploy, and they are built to expand with agencies as CDM moves into Phase 2 and beyond.

At IBM, the emphasis is on integration and expertise – ensuring that agencies and other clients have the products and solutions they need to make all the pieces work, no matter what IT environment they operate in.

Selfie

IBM's confidence in its solutions is evident by its own use of them. The company relies on endpoint management to provide a snapshot of its internal systems.

IBM uses its endpoint management to support more than half a million devices internally. And because the solution is so effective, it requires just three employees to manage the endpoint security program. That speaks to the limited maintenance that IBM's endpoint management requires, which is important to agencies with limited budgets.

Another View

IBM's $4 billion annual investment in cyber security and analytics has paid off. Forrester ranked IBM as a leader in information security consulting in 2013.

It also was named the leader in 2013 in Gartner's "Magic Quadrant for Security Information and Event Management" and the "Magic Quadrant for Client Management Tools" for its endpoint management capabilities.

That's what happens when you see the full picture.

Peter Allor
Security Strategist

RedSeal Networks – Mapping Networks, and Charting a Course for Cyber Defense

A tourist on a subway system understands the value of a good map.

Like a subway, an organization's computer network can seem vast and complex. Even well-traveled executives can find themselves wondering about the scale and complexity of the systems their IT teams have built.

RedSeal's Network Infrastructure Security Management System helps organizations understand, end to end, the topology of their infrastructure and every potential attack path. The solution helps executives and IT professionals find their way when they've lost sight of how far and wide their complicated networks extend.

Mapmakers at Work

Producing an accurate "map" starts with preparing a thorough model to represent all the paths a network takes. The key is knowing how far a network extends. Once the RedSeal solution determines the extent of an organization's computer network, the technological cartographers then identify all the other networks that it touches.

RedSeal's solution produces a single image to illustrate the model of the organization's network and its myriad connections to other networks.

Danger Ahead

Once the map is created, RedSeal has the ability to continuously monitor any changes that occur within a network so organizations are able to answer critical questions including:

- How secure is my network at this moment?
- What vulnerabilities should we fix first?

The solution also measures security and the potential danger from threats through a comprehensive "risk scoring" system that allows IT professionals, supervisors, and executives to visualize changes to their networks.

Reading the Signs

Practically, this gives an organization valuable real-time visibility to see potential risks their networks face and vulnerabilities that could be exploited. By proactively measuring risk, the solution gives the IT professionals on the front lines the ability to determine which risks require immediate attention because they are time critical.

Having this crucial information provides executives a risk management framework that enables improved decision making.

As part of its Joint Regional Security Stack, the U.S. Army recently awarded continuous monitoring to RedSeal, whose solution allows the military to see its network and determine on a daily basis what the impact of network changes on security are.

The RedSeal solution is easily integrated into existing network infrastructure and other security tools that may be implemented as part of an agency's continuous monitoring solution.

As agencies move forward with continuous monitoring solutions, understanding the size and scope of their networks today is a crucial first step.

It's tough to know what direction to turn if you don't know where you are.

Everybody needs a good map.

Kimberly Baker
Vice President Public Sector,
Sales & Business Development

RSA – Painting a Picture

When it comes to CDM, an effective data aggregation tool is good. An effective data analysis tool makes it better. RSA's Archer Continuous Monitoring Solution – a governance, risk, and compliance (GRC) solution – does both. RSA isn't new to the game. Numerous federal agencies including the Internal Revenue Service (IRS), Department of Energy (DOE), and DHS already use Archer GRC solutions. With agencies preparing for the first phase of DHS' CDM program, RSA is broadening its relationships with other agencies that it believes can also benefit from its GRC solution portfolio. Enabling visualization of a wide range of metrics, understanding risk, eliminating costly and burdensome manual security processes, supporting agency decision processes, and driving enhanced security are just a few of the ways RSA sees Archer adding additional value to the agencies.

Casting a Wide Net

Archer automatically collects vast amounts of data aggregated by the cyber security solutions agencies currently have deployed across their networks. Since Archer is technology agnostic, it doesn't matter which of the disparate CDM security tools agencies will use to collect data from hardware and software asset management, vulnerability scans, or configuration settings.

The GRC tool has the ability to continue aggregation and analysis in subsequent phases as CDM evolves and requirements change. Archer is also uniquely positioned to support future agency executive data aggregation, metrics, dashboard, and reporting needs in such areas as supply chain, continuity of operations, audits, incidents, enterprise risk, and many others. That resiliency will make Archer relevant throughout the life of the program, help agencies get the most value out of their massive investment in the cyber security tools they deploy, and boost their return on investment.

But aggregating data represents just part of the challenge agencies face.

Making Sense of the Data

Getting the greatest utility out of data requires understanding what the information means.

Archer allows agencies to quantify their risk by leveraging robust risk scoring functionality. That allows agencies not only to grasp the immediate risk associated with specific vulnerabilities, but also to help determine which risks they need to mitigate first as well as support trend and predictive analysis. The formulas used to determine the outcomes of those calculations are configurable and can be changed based on an agency's priorities and risk profile.

Archer also simplifies efforts to present information. Because seeing is believing, RSA's GRC solution illustrates data in a way that is easy for people at all levels to understand and, where appropriate, take immediate action. Visualizing risk allows agency executives as well as security specialists to digest information quickly and react in a timely manner to mitigate vulnerabilities, configuration issues and other security challenges.

This simplifies the efforts of the IT departments that must communicate their monitoring efforts to those throughout their agencies.

RSA has also automated the Assessment and Authorization process, potentially saving federal agencies millions of dollars by streamlining a labor-intensive effort.

Praise from Analysts

Technology analyst firm Gartner Inc. named RSA a leader in Enterprise, Governance, Risk, and Compliance Management for the third year in a row. Last year RSA also received leadership recognition in the Gartner 2013 MarketScope for IT Governance, Risk and Compliance Management and the new Gartner Business Continuity Management Magic Quadrant.

Looking Ahead

RSA already is looking to the future. It is committed to empowering agencies to go beyond a passive posture of reacting to threats. RSA's cyber governance and cybersecurity solutions allowing them to predictively secure their IT infrastructure. This will give them the power to strengthen their networks and reduce risk by anticipating potential future attacks.

With RSA, agency IT leaders can take their data aggregation and analysis capabilities to the highest level.

Dan Carayiannis
Security Strategist

Symantec – Helping Agencies Manage Risk

Agencies already wade through a flood of data. When DHS' CDM program starts to mature, the flood will turn into a data tsunami.

Navigating those waters will require more than a paddle – it will demand special skill and a well-thought out strategy.

Symantec Corp.'s Control Compliance Suite is a critical solution that gives agencies a framework on which to build their governance, risk, and compliance (GRC) programs.

The solution – like continuous monitoring itself – has long been part of a comprehensive cyber security defense strategy. Private sector companies in healthcare and financial services industries, to name a few, have used the Control Compliance Suite (CCS) for more than a decade. And in that time, Symantec has continued efforts to innovate and improve its GRC tool.

A Clear View

Managing the waves of data will be as crucial as ever. To accomplish that, agencies will need the enterprise-wide visibility that Symantec's risk and compliance tools provide. With that visibility, agencies are able to see all of their network's vulnerabilities, determine the risk posed by specific threats, and figure out which threat they need to mitigate first.

The ability to visualize risk provides other benefits.

The automated system allows agencies to produce and share compliance data in real time. It also helps IT departments communicate the risks throughout an agency. Discussions about cyber security and threats to data and networks no longer are limited to the IT department. Leadership is engaged in these important discussions, and CCS allows IT to convey important information about risk in an easy to understand format.

Symantec's data aggregation is the key element that makes it all work.

For Today and Tomorrow

While agencies are focused on Phase 1 of the CDM program now, it is worth noting that CCS will remain relevant throughout the life of the project – all phases and all functional areas. As future phases come online, agencies will add more tools and sensors as part of their monitoring solution. Symantec's CCS solution can remain the central repository – the backbone – for the output produced by those additional tools.

That's because CCS works even if an agency has installed sensors made by a company other than Symantec. The CCS solution's ability to aggregate data means there's no need to rip and replace other tools.

Standing Up. Standing Out.

Symantec established its bone fides in the technology sector well ahead of the pack.

Norton Anti-Virus Software elevated the company's profile, but Symantec's Global Intelligence Network (GIN) represents the crown jewel that helped establish its industry-wide credibility. In fact the GIN plays a significant role in Symantec's CDM efforts. Symantec uses data gathered by the GIN to bolster CDM efforts. Understanding the vulnerabilities and attacks that occur elsewhere help protect the data and network of Federal agencies.

Its comprehensive security tools and vast experience make Symantec a successful CDM solution provider. And that's good for Federal agencies in search of a governance, risk, and compliance solution to navigate the flood of data that CDM will generate.

Kenneth Durbin
Continuous Monitoring &
Cyber Security Practice Manager

Jennifer Nowell
Senior Director,
Strategic Programs

Tripwire – Perfect Vision

Tripwire enables organizations to see things other solutions don't. Their solutions deliver unparalleled risk visibility, business context, and system state intelligence to more than 7,000 customers globally. This allows enterprises to continuously protect data and assets from breaches, vulnerabilities, and threats through: Security Configuration Management, Vulnerability Management, File Integrity Monitoring, and Log & Event Management

Comprehensive Scanning

Tripwire's solutions continuously assess network assets. The company's configuration management tool monitors in real time, quickly locating and remediating non-compliant configurations.

Its vulnerability management tool provides clients with in-depth analysis, refreshing data as often as every 24 hours, collecting critical information about vulnerabilities.

Tripwire's hardware and software asset management solutions provide great detail about network assets so clients have a clear picture of the scope and scale of their networks.

Tripwire has deployed these capabilities on Federal agency networks of all sizes to provide lock-down security. Automation reduces the typical burden on security staff, and a self-service portal allows everyone with system responsibilities to access just the data they need.

Meaningful Data

Tripwire's ability to collect timely data about assets, vulnerabilities, and configurations represents a huge advantage for clients. Its skill in turning system state information into actionable intelligence provides even greater value.

Tripwire prioritizes the potential impact of vulnerabilities so clients know where to focus remediation efforts, with many agencies reducing their exposure to cyber threats by 80 percent within 18 months of implementation.

Superior Results

A testament to the company's longevity in the risk-based security and compliance management space, the U.S. Agency for International Development has used Tripwire's continuous monitoring solution since 2005.

The Centers for Medicaid and Medicare Services (CMS) in 2012 earned recognition for its monitoring efforts. Using Tripwire, CMS received a Best Practice Award for efforts to reduce risk by 80 percent at 88 data centers. At one major data center, CMS reduced risk by 95 percent.

And the leading Federal auditing agency has leveraged Tripwire monitoring for cyber security efforts, FISMA compliance, and integration into their Certification & Accreditation (C&A) process, allowing the agency to save an estimated $1.8 million.

Last year, NIST's National Voluntary Laboratory Accreditation Program gave Tripwire the Security Content Automation Protocol (SCAP) 1.2 designation – making it the only security vendor to achieve that validation.

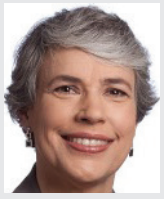
Tripwire's solutions also are modular, so agencies that already have a program investment in another vendor don't need to rip and replace to bring in a Tripwire solution.

Focused on Results

Perfect vision is rare. Agencies have difficulty seeing across networks to see the impact of vulnerabilities, remediate configuration issues, and inventory assets.

But Tripwire hasn't lost its focus. They deliver the automation to secure complex network infrastructures and give organizations confidence.

John Klein
Federal Sales Director



Keren Cummins
Field Sales

Thank You

We would like to thank the following individuals for their valuable insight:

Wasif Shakeel
Senior Director for Continuous Monitoring and Diagnostics and Cyber Security Services Health and Civilian Solutions Division
General Dynamics Information Technology
wasif.shakeel@gdit.com
(202) 596-0060

Ed Keegan
Director, Cybersecurity Solutions Group Portfolio
HP Enterprise Services, U.S. Public Sector
edward.keegan@hp.com
(719) 696-4145

Gregg Hawrylko
CDM/CMaaS BPA Program Manager
HP Enterprise Services, U.S. Public Sector
hawrylko@hp.com
(703) 733-3008

Peter Allor
Security Strategist
IBM
pallor@us.ibm.com
(404) 643-9638

Kimberly Baker
Vice President Public Sector, Sales & Business Development
RedSeal Networks
kbaker@redsealnetworks.com
(410) 310-3336

Dan Carayiannis
Security Strategist
RSA
dan.carayiannis@rsa.com
(703) 304-2497

Kenneth Durbin
Continuous Monitoring & Cyber Security Practice Manager
Symantec Corporation
kenneth_durbin@symantec.com
(301) 526-8213

Jennifer Nowell
Senior Director, Strategic Programs
Symantec Corporation
jennifer_nowell@symantec.com
(301) 526-8213

John Klein
Federal Sales Director
Tripwire
jklein@tripwire.com
(703) 421-4529

Keren Cummins
Field Sales
Tripwire
KCummins@tripwire.com
(301) 379-2493

Cindy Auten
General Manager
MeriTalk
cauten@meritalk.com
(703) 489-1185