carahsoft

govloop

YOUR GUIDE TO

Mission-Driven Cybersecurity

Contents

3 Introduction

4 Carahsoft's FedRAMP Solutions Providers

7 Enterprise Integration Platform Accelerates Modernization

8 The State of Cybersecurity in Government Today

11 In Lieu of a Perimeter, Put Security at the Edge

12 The Case for Mission-Driven Cybersecurity

15 Why Network Visibility Is Key to Business Continuity

16 Destination: Zero Trust?

19 Observability Platforms: Because App Monitoring Is Not Enough

20 TIC Gets Agile

23 The Cloud Era Requires Cloud-Ready Cyber Policies

24 CDM Keeps Eye on Shifting Cyber Requirements

27 Identity Emerges as Key Piece of Modern Cybersecurity

28 FedRAMP Responds to Agency, Industry Pain Points

31 Evolving Cyber Policies Clear Way for Cloud Adoption

32 Best Practices in Federal Cybersecurity

35 Intelligent Network Visibility Serves as Security Force Multiplier

36 TIC 3.0 Starter Kit

39 Why a People-Centric Approach to Security Has Become a Necessity

41 Why the Future of Security Is Cloud Native

42 Conclusion, About and Acknowledgments

Carahsoft and GovLoop have partnered to provide resources around the latest federal IT initiatives and legislation. The goal is to guide government leaders and stakeholders interested in learning more about procurement initiatives and the solutions available through them.

Introduction

Over the years, the federal government has created a series of mandates to push agencies toward adopting better cybersecurity practices and solutions. The goal is not to define a one-size-fits-all security strategy across government, but to provide a good foundation on which agencies can build.

Today, three such mandates guide most agency efforts: **the Federal Risk and Authorization Management Program (FedRAMP)** for cloud security; the **Continuous Diagnostics and Mitigation (CDM)** program for network visibility and data security; and the **Trusted Internet Connections (TIC)** program for internet-based security.

The mandates were developed largely independent of one another, yet increasingly they are seen as interlocking pieces of a larger puzzle. That puzzle is this:

How can agencies create a more agile IT environment — one that evolves as mission requirements evolve — without compromising the security of their networks, systems and data?

This guide, created by GovLoop and Carahsoft, looks at that puzzle. We focus both on the individual mandates — FedRAMP, CDM and TIC — and how they interrelate. We also look to the future: How are these mandates themselves evolving, how will that shape the future of federal cybersecurity efforts, and how will those efforts help support agency missions?

Like the mandates, this guide does not provide a definitive answer to those questions. But we hope that it contributes to the broader discussion about what mission-driven cybersecurity means.

Carahsoft's FedRAMP Solutions Providers

More than 90 FedRAMP solutions are available through Carahsoft and its reseller partners, enabling agencies across Federal, State and Local Government to access a wide range of cloud-based technologies to securely drive modernization and digital transformation.

Accellion	Kiteworks Federal Cloud
Acquia	Acquia Cloud
Adobe	Adobe Analytics Adobe Campaign Adobe Captivate Prime Adobe Connect Managed Services (ACMS-GC) Adobe Creative Cloud for Enterprise Adobe Document Cloud (PDF Services & Adobe Sign) Adobe Experience Manager Managed Services (AEMMS-GC)
Akamai	Content Delivery Services
APPTIO	The Apptio Technology Business Management (TBM)
aws partner network	AWS GovCloud AWS US East/West
AXON	Axon Evidence.com
axway	Syncplicity Federal Government
BlackBerry	BlackBerry Cloud - AtHoc Services for Government BlackBerry Government Mobility Suite
BlackBerry CYLANCE	CylancePROTECT
box	Box Enterprise Cloud Content Collaboration Platform
BROADCOM	Clarity PPM General Support Systems (GSS)
CloudCheckr	CloudCheckr Federal
COFENSE	Cofense PhishMe

CONTEGIX	SecureCloud
DATADOG	Datadog
DECISION LENS	Decision Lens Software
boomi	AtomSphere
DocuSign	DocuSign Federal
druva	Druva inSync
exterro	Exterro E-Discovery and Legal Software Platform
FIREEYE	FireEye Email Security GovCloud
Google Cloud	Google G Suite Google Services (Google Cloud Platform Products and Underlying Infrastructure)
GRANICUS	GovDelivery Communications Cloud
ivanti	Ivanti Service Manager
Lookout	Lookout Mobile Endpoint Security
McAfee	MVision Cloud MVision Cloud - JAB MVision for Endpoint
MICRO FOCUS Government Solutions	Fortify on Demand
Microsoft	Azure Commercial Cloud Azure Government Dynamics 365 for Government Office 365 Multi-Tenant & Supporting Services Microsoft Office 365 GCC High

MuleSoft	MuleSoft Government Cloud
netskope	Netskope OneCloud Government
New Relic.	New Relic
NUTANIX	Nutanix XI Government Cloud
okta	Identity as a Service (IDaaS)
paloalto NETWORKS	Palo Alto Networks Government Cloud Services – Prisma Access Palo Alto Networks Government Cloud Services - WildFire Palo Alto Networks Government Cloud Services ZingBox IoT Guardian
proofpoint.	Proofpoint Email and Information Protection Service Proofpoint Email Archive Proofpoint Targeted Attack Protection Proofpoint Security Awareness Training
qualtrics EXPERIENCE MGMT	Qualtrics XM Platform
Qualys.	Qualys Cloud Platform
rackspace.	Rackspace Government Cloud
SailPoint	IdentityIQ
salesforce	Salesforce Government Cloud Salesforce Government Cloud - JAB MuleSoft Government Cloud
NS2	SAP NS2 Cloud Intelligent Enterprise SAP NS2 Secure Node with SuccessFactors Suite - DoD Qualtrics XM Platform
SAVIYNT	Saviynt Security Manager

servicenow	Government Community Cloud Service Automation Government Cloud Suite (Legacy)
slack	Slack
smartsheet	Smartsheet Gov
snowflake	The Snowflake Service on AWS The Snowflake Service on Azure Government
Socrata	Socrata Data Platform
software AG GOVERNMENT SOLUTIONS	Software AG Government Cloud
splunk>	Splunk Cloud
springcm	SpringCM
Symantec.	Symantec Web Security Service (WSS) Government
VALIMAIL	Valimail Enforce Platform
VERITONE.	aiWARE Government
virtru	Virtru Data Protection Platform
virtustream	Federal Cloud (VFC)
vmware	Airwatch by VM Government Services (AGS) Workspace ONE VMware Cloud on AWS GovCloud (VMC)
zoom	Zoom for Government
zscaler	Zscaler Internet Access – Government (Secure Web Gateway - vTIC) Zscaler Private Access - Government (Zero Trust Networking - VPN Replacement) Zscaler Private Access - Government (Zero Trust Networking VPN Replacement) - JAB

Carahsoft's FedRAMP solutions are available through its reseller partners on a variety of contracts including Carahsoft's GSA Schedule 70, SEWP V, ACCENT, NASPO ValuePoint, and numerous state and local contracts. To learn more, contact us at (703) 871-8646 or visit Carahsoft.com/FedRAMP.

boomi

A Dell Technologies Business

Accelerate Mission Outcomes

Modernize and transform to create seamless and connected government experience

Learn More

INDUSTRY SPOTLIGHT

Enterprise Integration Platform Accelerates Modernization

An interview with Alan Lawrence, Vice President, Dell Boomi Federal

One of the most pressing IT issues in most agencies is the concept of technical debt, with agencies continuing to be constrained by their reliance on outdated legacy systems. They would like to wipe out that debt by adopting more modern platforms, but they struggle to make that transition. How can they bridge that gap between legacy systems and modern platforms?

That's where the concept of integration platform as a service comes in. iPaaS is a cloud-based service that integrates applications, data and processes across different cloud and on-premises platforms. Although iPaaS might be new to many agencies, it has been in use in the commercial sector for more than a decade.

To learn about iPaaS, GovLoop spoke with Alan Lawrence, Vice President for Federal at Boomi, a Dell Technologies company. Lawrence identified three key use cases for iPaaS.

Rationalizing, consolidating applications

When it comes to modernization, agencies understand the need for application rationalization – that is, taking stock of their existing applications and determining which still deliver value and which should be consolidated or simply shut down. The challenge is to ensure that critical data is not lost in the process.

That's where iPaaS comes in. iPaaS ensures a smooth transition with reliable data exchange between the original application and the new platform. With iPaaS, "you can actually decommission a whole crate of applications, taking the time you spent on maintenance and moving it to something else," Lawrence said.

Because iPaaS is cloud-based, FedRAMP authorization is a must. With FedRAMP-based security, agencies can integrate data in a trusted and secure environment that supports data quality, governance and compliance.

Accelerating the move to the cloud

Increasingly, agencies are choosing to move applications from a legacy system to a cloud platform. Traditionally, that would require an intensive, drawn-out effort by programmers to map out all the different points of integration. But with iPaaS, that's not the case.

Boomi's iPaaS platform, for example, includes an algorithm driven by artificial intelligence that suggests how to handle complex data mapping, which is a critical but often time-consuming part of integration configuration. From Boomi's experience, the algorithm is 92% accurate – meaning that the IT staff can focus on addressing the remaining 8%, Lawrence said.

The platform also provides a low-code, drag-and-drop interface that is designed to be used by the "business" owners, who have the best understanding of operational requirements, he said.

Connecting with outside services

Another challenge is moving data from an on-premises system to a cloud-based one – for example, from SAP to SAP Hana, Remedy to ServiceNow, or PeopleSoft to WorkDay – with data transformation required in the middle.

Agencies often have to start from scratch when they make that first transition, because the original data integration was done 20 or 25 years ago and was never documented. An iPaaS provides a fresh start. As the new data integration is designed, the platform captures it in a Visio-like diagram.

"You end up with a diagram of literally every integration you're doing – where the data is coming from, where it is going and what is happening to it in the middle," Lawrence said.

The State of Cybersecurity in Government

31,107

Cybersecurity incidents in the federal government in fiscal 2018

$14.98 billion

Cybersecurity spending in the federal government in fiscal 2018

Source: OMB

Remember When...?

A 2007 memorandum by then-OMB Director Clay Johnson III first articulated the TIC policy. This was just a few years before the federal government would adopt the Cloud First policy, which eventually would render the original TIC vision wholly impractical. Here is how the memo began:

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

DEPUTY DIRECTOR
FOR MANAGEMENT

November 20, 2007

M-08-05

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

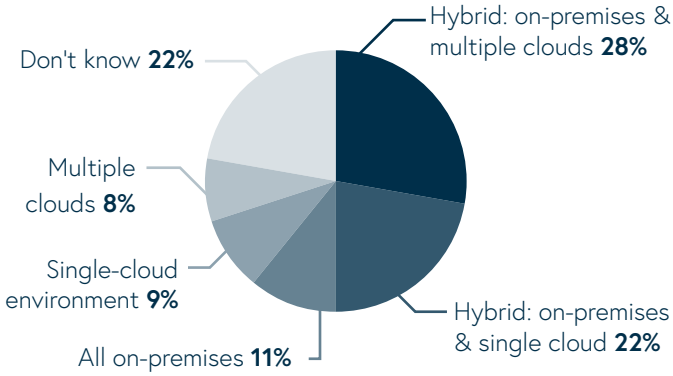
FROM: Clay Johnson III

SUBJECT: Implementation of Trusted Internet Connections (TIC)

I am announcing the Trusted Internet Connections (TIC) initiative to optimize our individual network services into a common solution for the federal government. This common solution facilitates the reduction of our external connections, including our Internet points of presence, to a target of fifty. Additionally, the role of the US-CERT will be enhanced to improve our response capabilities. Each agency will be required to develop a comprehensive plan of action and milestones (POA&M) with a target completion date of June 2008. Initial agency POA&Ms must be sent to the Department of Homeland Security's (DHS's) National Cyber Security Division (NCSD) by January 8, 2008, for review and agreement with OMB, DHS, and the agency.

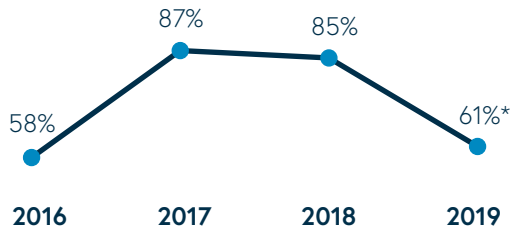
Complexity on the Rise

In a 2019 survey of federal IT officials, only 11% of respondents said that all their agency's applications would reside on-premises once modernization is complete. In contrast, about 50% said their agencies were moving to a hybrid environment, and more than half of those said their agency would use multiple clouds.



Mandates Make a Difference

A February 2020 report from the Government Accountability Office (GAO) correlated cyber improvements with cyber mandates. For example, a 2015 directive on critical vulnerability mitigation required agencies to address within 30 days critical vulnerabilities discovered by cyber scans of internet-accessible systems. Here is the percentage of cases in which agencies met that requirement:



**GAO said the drop in 2019 was attributed to the government shutdown.*

The History of Zero Trust in the Federal Government

The concept of zero trust cybersecurity might be unfamiliar to many people in the federal IT community, but it actually has a long history in government, according to the National Institute of Standards and Technology (NIST). In the February 2020 draft of NIST Special Publication 800-207, "Zero Trust Architecture," NIST identified four key milestones in the evolution of this cyber model:

- The work of the Jericho Forum in **1994** publicized the idea of de-perimeterization — limiting implicit trust based on network location and the reliance on a single, static defense over a large network segment.
- The Defense Information Systems Agency and the Defense Department published their work on a securer enterprise strategy dubbed "black core" (circa **2007**). Black core involved moving from a perimeter-based security model to one that focused on the security of individual transactions.
- The concepts of de-perimeterization improved and evolved into the larger concept of zero trust, a term John Kindervag coined in **2010** while at Forrester Research. Zero trust then became the term used to describe various cybersecurity solutions that moved security away from implied trust based on network location and instead focused on evaluating trust on a per-transaction basis.
- Federal agencies have been urged to move to security based on zero trust principles for more than a decade, building capabilities and policies such as the Federal Information Security Modernization Act (FISMA), followed by the Risk Management Framework; Federal Identity, Credential and Access Management; TIC; and CDM programs. All aim to restrict data and resource access to authorized parties.

Cloud-Based Concerns

In a 2019 survey, GovLoop asked federal, state and local employees to select their biggest security concerns around cloud/hybrid solutions. Here is what they said:

62%
Data security/privacy

62%
Application performance & availability

42%
Lack of qualified personnel in the agency to manage the environment

26%
Inability to monitor & troubleshoot applications

Increase Your Agency's Agility and Reduce Risk

Zscaler meets the TIC 3.0 framework to speed and secure your agency's digital transformation

To successfully move applications to public and private clouds, you need to modernize your security architecture. A zero trust approach eliminates the attack surface exposed by legacy technologies and enables an agile, remote workforce. The Zscaler™ multitenant cloud security platform meets the TIC 3.0 framework with fast, secure connections to the internet, SaaS, and internal applications.

Agencies are choosing Zscaler to:

Improve user experience – users simply connect to their applications regardless of their location or device; no latency caused by backhauling

Reduce risk – delivers consistent protection no matter where users connect or what devices they're using

Enhance security – connections to SaaS and internally managed applications are based on agency policies

Modernize IT – fosters agility while eliminating the cost and complexity of security appliances

Reduce costs – no hairpinning through MTIPS or the legacy TIC perimeter, no appliances

Secure shared services – eliminates the need for security stacks, increases efficiencies

LEARN MORE ABOUT THE ZSCALER FEDRAMP-AUTHORIZED CLOUD PLATFORM.
zscaler.com/government

FedRAMP *authorized*

INDUSTRY SPOTLIGHT

In Lieu of a Perimeter, Put Security at the Edge

An interview with Stephen Kovac, Vice President of Global Government and Compliance, Zscaler

The rise of cloud, mobility and related applications effectively have undermined the concept of perimeter-based security. That is why TIC 3.0 addresses the need to address security when users, applications and data reside outside the perimeter.

The secure access service edge (SASE) security model is the next logical step. SASE pushes IT services and associated security measures from the perimeter out to the edge, delivering them through the cloud.

To learn more about SASE, we spoke with Stephen Kovac, Vice President of Global Government and Compliance at Zscaler, which operates a multitenant distributed cloud security platform. He highlighted three key benefits.

Reduced IT cost and complexity

In a traditional network environment, IT and security services operate within the data center. That was manageable when end users and IT services worked within the perimeter. But as agencies have accelerated their adoption of cloud and mobile solutions, the traditional approach has proven increasingly difficult to scale, since it requires everything to get rerouted back to the data center.

SASE changes that model by extending IT and security services to wherever end users, systems and data reside, reducing the burden on the network and the data center, and making it easy to scale as new requirements emerge.

It also reduces data center bloat. "The idea of having these big multiple stacks in the data center – and having to update and maintain that equipment – goes away, because now it's being done in the cloud," Kovac said.

Better user experiences

Another challenge of working in a widely distributed environment is that the user experience becomes unpredictable. In the traditional network environment, users and systems outside the data center typically rely on a virtual private network (VPN) to connect to the network securely, with variable levels of performance.

By pushing security services closer to the user or system – and by connecting users or systems directly to cloud applications and services – SASE ensures optimal bandwidth and low latency.

This model also provides a consistent experience as a user moves from one location to another. Whether that user is working out of an office in Washington, D.C., from home, or at a remote location, they will have the same experience and better performance, Kovac said.

Reduced risk

By design, SASE integrates wide area networking and security capabilities. This ensures that all connections are inspected and secured, no matter where the user or system is or what application is being accessed. And SASE provides a zero trust network access (ZTNA) model, providing connectivity only if the user or system is authorized to do so.

SASE is a cyber version of social distancing. By moving security services out to the edge, an agency keeps users and services from getting inside the perimeter. And by shielding the network and IPs from the internet, SASE helps move agencies closer to a zero attack surface, Kovac said.

"How do you achieve that idea of no perimeter and no attack surface, but still deliver services? We have been caching and accelerating data at the edge for years. This evolution now allows us to compute and secure at the edge. That's what SASE is," Kovac said.

The Case for Mission-Driven Cybersecurity

As agencies increasingly rely on online resources to execute their missions, they must fully integrate cybersecurity into networks, platforms and applications to enable cybersecurity to become a mission enabler.

The model for securing government information resources has changed radically in the past 70 years. With the first standalone computers in the 1940s, it was primarily a matter of physical security. The advent of networking made cybersecurity an issue, addressed with add-ons that users too often saw as inhibitors.

But in an era of ubiquitous connectivity, increased complexity and the elimination of the network perimeter, cybersecurity is being integrated throughout the information infrastructure to become a mission enabler. This integration simplifies security, making it more efficient and effective. It supports the adoption of rapidly evolving technologies such as the cloud and mobile computing, allowing for better delivery of information and services to government users and the public.

The reliance on online resources that agencies need to complete missions requires a seamless cybersecurity defense. And cybersecurity itself has gone from focusing on the prevention of malicious activities to being an active element in making the IT architecture reliable, accessible and secure.

Adopting and Adapting

Building effective cybersecurity into IT systems enables visibility throughout the network and out to all of its endpoints, allowing implementation of granular controls for devices. In the past decade, the federal government has developed policies to help agencies implement the tools and services they need.

FedRAMP: Cloud computing is replacing static, proprietary systems with flexible commercial platforms for the rapid deployment of resources. In 2011, the federal government adopted a cloud-first strategy, followed the next year by FedRAMP.

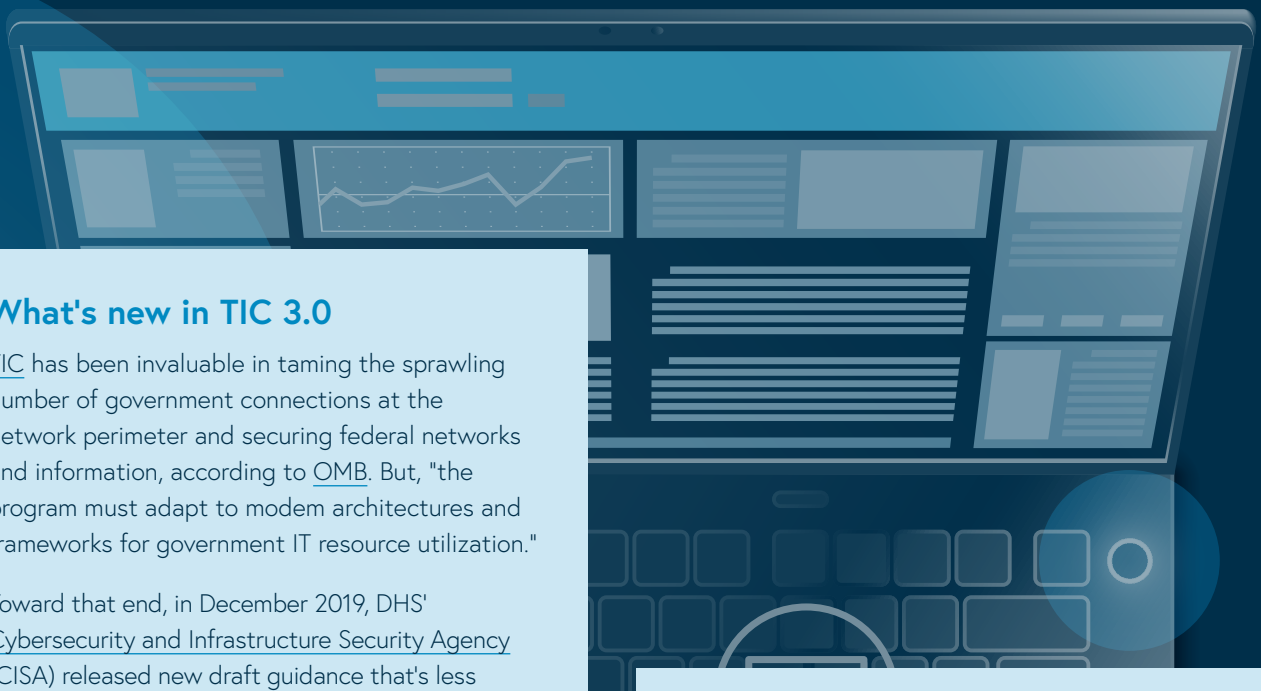
FedRAMP's purpose is to simplify and improve the assessment of service provider security with a "do once, use many times" approach. Today the FedRAMP Marketplace has has 182 offerings, with another 52 in process, 30% of them added in fiscal 2019, and the FedRAMP process is being automated to improve efficiency.

CDM: Continuous monitoring and reporting is replacing the original FISMA security standard of periodic assessment for IT systems. To enable this, the Homeland Security Department (DHS) established CDM in 2012, making commercial tools and services easily available.

According to CDM Program Manager Kevin Cox, the initiative has increased IT visibility so that agencies can discover, on average, 75% more devices on their networks. CDM's original blanket purchase agreement on the General Services Administration's IT Schedule 70 expired in 2018 and has been replaced by an updated acquisition strategy using GSA Special Item Numbers for CDM products and services. This change allows for new offerings to be quickly added to the program.

TIC: The initial goal of TIC was to reduce the number of federal internet connections from 4,000-plus to a more manageable and secure 50 or so. Consolidating outside connections and deploying a common set of tools have helped improve security, but TIC has evolved along with government architectures.

In September 2019, OMB announced plans for TIC 3.0 as a way to provide "increased flexibility to use modern security capabilities" and ensure that the program can evolve as needed. Drafts of updated guidelines for Version 3.0 were issued in December 2019, and public comments are being reviewed before the final implementation.



What's new in TIC 3.0

TIC has been invaluable in taming the sprawling number of government connections at the network perimeter and securing federal networks and information, according to OMB. But, "the program must adapt to modem architectures and frameworks for government IT resource utilization."

Toward that end, in December 2019, DHS' Cybersecurity and Infrastructure Security Agency (CISA) released new draft guidance that's less focused on the perimeter and intended to accelerate agency adoption of the cloud, mobile computing, strong encryption and other emerging technologies. This gives more flexibility to agencies in selecting and acquiring new technology to let each meet its unique security needs.

The updated policy allows the agencies to assume broader interpretation authority. TIC 3.0 accommodates a wide variety of scenarios, and the guidance has a different tone and level of detail compared with earlier versions to accommodate this increased selection. Agencies will use the TIC 3.0 Program Guidebook, Reference Architecture, and Security Capabilities Handbook (all available here) to determine how to protect their environments to conform with their risk management strategies and to address the security considerations outlined in the Use Cases document.

CISA plans to release final TIC 3.0 guidance in spring 2020.

(See interview with Sean Connelly, TIC Program Manager, on p. 20.)

CDM and the cloud

As federal agencies take advantage of the cost and time savings and flexibility cloud offers, they are redefining what constitutes their network environment. It is no longer enough to focus on locally managed networks and on-premises systems to meet the security requirements of continuous monitoring and reporting. DHS's CDM program is evolving to provide the products and services agencies need to meet these demands.

CDM originally addressed the management of agency devices and software. Phase 2 of the program expanded to include network users through management of account access, user privileges, credentials and authentication. Phase 3 addresses data, network perimeter components and user activity to ensure security throughout the agency's infrastructure, wherever it is.

This shift beyond the network perimeter requires visibility into the cloud and is not necessarily easy. Kevin Cox, DHS CDM Program Manager, said the initiative is going beyond on-premises networks to get additional visibility through Dynamic and Evolving Federal Enterprise Network Defense (DEFEND), which provides task orders supporting cloud and mobile cybersecurity. Use of FedRAMP-approved security solutions on the CDM Approved Product List can also help provide visibility and management capabilities in the cloud.

(See interview with Kevin Cox on p. 24.)

FOUNDATIONAL SECURITY, SIMPLIFIED

Protect Your Organization and Investigate Threats Faster

REDUCE RISK using a scalable ubiquitous cybersecurity platform

IMPROVE ORCHESTRATION of your security tools

AUTOMATE threat investigation and hunting

Learn how at:
infoblox.com/solutions/government/

Infoblox® FEDERAL

INDUSTRY SPOTLIGHT

Why Network Visibility Is Key to Business Continuity

An interview with Chris Usserman, Principal Security Architect, Infoblox Federal

When the COVID-19 crisis forced many federal employees to start working from home, agency IT leaders found themselves in a new environment—employee living rooms. They quickly realized that while their business continuity plans address key issues around connectivity, security at this scale has proven to be something of an afterthought.

What are the critical security concerns that agencies need to incorporate into their business continuity plans going forward? To answer that question, GovLoop spoke with Chris Usserman, Principal Security Architect at Infoblox Federal, a provider of on-premise and cloud-managed network/security services.

Not part of the plan

What's often missing is a security strategy that provides holistic visibility of what's happening at the endpoint. Agencies often have that capability within the network perimeter, but ***"they never planned for everyone's home router to take the place of the hundreds of thousands of dollars they've invested in perimeter defenses in their brick-and-mortar shop," Usserman said.***

Most agencies provide employees with connectivity through virtual private networks (VPNs), but that can create a false sense of security. People often assume that if they are accessing agency resources through a VPN, then security controls are in place. But a VPN only secures the transport layer, not the information being transmitted within. Malware can communicate through, and in spite of, a VPN since it can affect systems at the kernel layer of the operating system. Malware doesn't have to follow normal software cooperation rules like "don't communicate directly to the internet when the VPN is active." Malware writes its own rules.

And consider this: When an employee connects a work laptop to the home network, it likely shares that network with everything from gaming systems, smart televisions and countless peripherals. To what extent does the agency have visibility into that environment and the vulnerabilities and threats that are already present?

Continuous monitoring revisited

Over the years, the Continuous Diagnostic and Mitigation (CDM) program has helped agencies to understand the importance of having visibility into everything happening on the network.

This is challenging enough when agencies are focused on devices and traffic within the network perimeter. What happens when the workforce is off premises for weeks or months at a time? Agencies need to ensure that they can maintain visibility in this distributed work environment – and have the ability to respond to threats in a timely manner.

With that in mind, Infoblox provides agencies with the following capabilities:

- Fortifying cloud access to extend headquarters protection to workers at home, including automatically detecting and blocking malware
- Protecting agency data by automatically blocking data exfiltration attempts and by detecting the security state of all connected devices
- Keeping employees safe from bad destinations and restricting access to web content not in compliance with agency policy
- Using early detection and threat intelligence to detect security threats quickly and to identify which threats require immediate attention

Network and threat intelligence is key to holistic visibility. The security operations center will detect countless threats each day. How do they determine which ones to make a priority? "It is essential to have tools that provide you with the right contextual visibility in a timely manner so that you can take action," Usserman said.

Destination: Zero Trust?

TIC 3.0, CDM, and other federal cyber initiatives and trends might signal a broad move to a zero trust security model.

Zero trust security architecture is finally getting traction in the federal government as agencies begin to realize that this concept — first formally defined 10 years ago — might be just what they have been looking for all along.

An analyst at Forrester first articulated the concept of zero trust in 2010. Zero trust recognizes that the growing adoption of cloud, mobility and related technologies have made the network perimeter incredibly porous. Rather than simply defending the perimeter, organizations should create additional layers of security enterprisewide.

Cloud and mobility threaten to "stretch traditional perimeter-based cybersecurity approaches to the breaking point," according to a 2019 report on zero trust from the American Council for Technology and Industry Advisory Council (ACT-IAC).

"Unless these deficiencies and challenges are addressed effectively and expeditiously, the government will be unable to properly protect our national assets and realize the potential benefits technology advances offer," the report states.

At a high level, zero trust entails putting security controls at the level of individual systems, applications and data — or any other network resource. Every time a user attempts to access a resource, the network should verify the identity of both the user and device and that both have permission to access that resource (authorization).

In other words, traditional security is like locking the front door to your house — people need a key to get in, but once in, they can roam freely. Zero trust is more like an apartment building in which the front entrance and all individual apartments are locked. It's not "trust but verify"; it's just "verify."

Looking for a quick tutorial on zero trust? Check out GovLoop's explainer video here.

The Principles of Zero Trust

In the February 2020 draft of NIST SP 800-207, NIST identifies seven basic tenets of a zero trust architecture.

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy — including the observable state of client identity, application and the requesting asset — and may include other behavioral attributes.
5. The enterprise ensures that all owned and associated devices are in the most secure state possible and monitors assets to ensure that they remain in the most secure state possible.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current state of network infrastructure and communications and uses it to improve its security posture.

Source: NIST

One challenge with zero trust is that there is no zero trust "solution" on the market. A zero trust architecture builds on multiple technologies and strategies (see below). But TIC 3.0 and CDM each provide some of the building blocks of zero trust.

In a draft report on zero trust architecture, NIST notes that many TIC 3.0 security capabilities — such as encrypted traffic, default/deny, virtualization security, network and asset inventory — directly support zero trust. More generally, TIC 3.0 supports the definition of different "trust zones" within a network, enabling an agency to apply different security controls to specific applications, services and environments.

CDM, on the other hand, provides the tools and processes needed to get better visibility into the network, according to NIST. That includes the ability to authenticate the individuals and devices connected to the network and to verify which resources they may access.

In November 2019, the NIST National Cybersecurity Center of Excellence and the Federal CIO Council hosted a two-day technical exchange on zero trust involving both government and industry. Participants provided feedback on the draft publication, discussed zero trust cybersecurity requirements, and shared best practices and lessons learned.

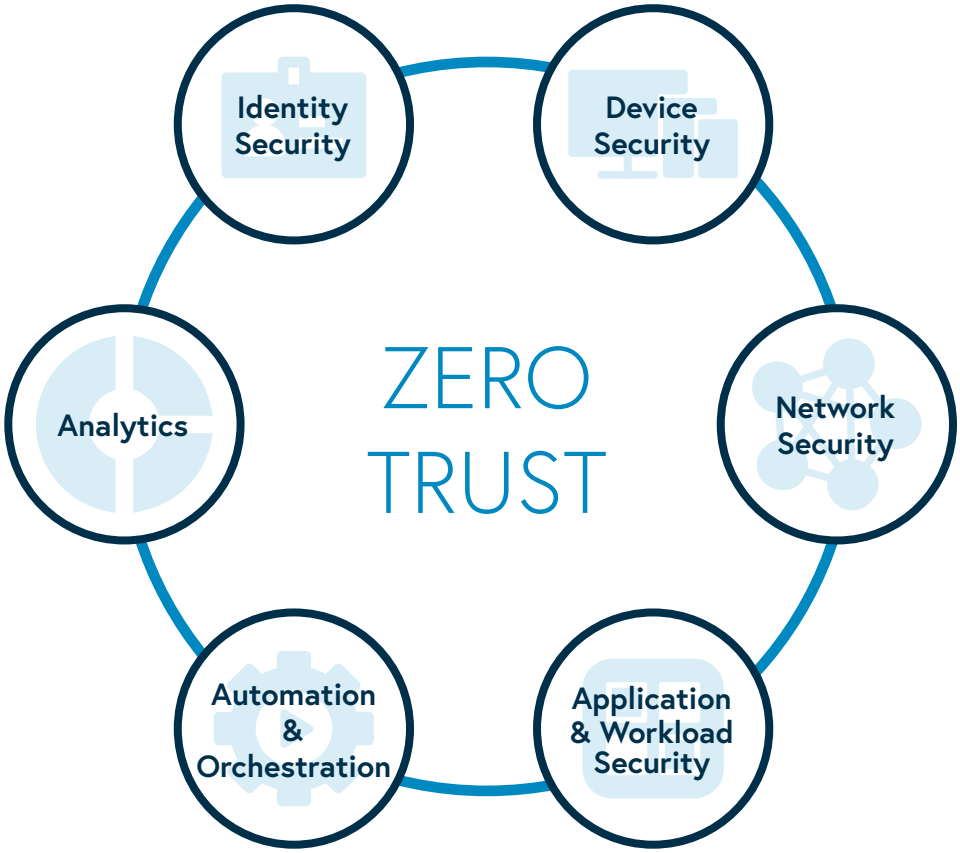
The TIC program office is seeing a lot of interest in zero trust, said Sean Connelly, TIC Program Manager at CISA.

"Usually when we build out a use case, we use one or two agencies and their pilots to build the use case," Connelly said. "But we suspect there's such momentum with zero trust, and there's so many different solutions to meet it, that we may need a number of pilots to support it. So, I would suspect we may have more than a handful of agencies doing zero trust pilots." (Read an interview with Connelly on p. 18.)

Six Pillars of a Zero Trust Security Model

In a 2019 report, ACT-IAC identified six key technology components of a zero trust architecture →

The report notes that data is the foundation of a zero trust architecture. To understand what they are protecting and the risks involved, "organizations need to categorize their data assets in terms of mission criticality and use this information to develop a data management strategy as part of their overall [zero trust] approach."



New Relic®

Data-driven insights that improve digital citizen experience and optimize cloud usage

New Relic is the only FedRAMP-authorized programmable observability platform

---

New Relic uniquely delivers agency stakeholders needed visibility and understanding of their IT-driven customer experiences, business operations, and IT applications, and presents it in a meaningful, customizable, and easily digestible way that caters to any stakeholder.

We instrument, measure, and improve public sector applications and hybrid infrastructures to help agencies create better-performing software, experiences, and mission-supporting IT.

Visit us at newrelic.com/public-sector

INDUSTRY SPOTLIGHT

Observability Platforms: Because App Monitoring Is Not Enough

An interview with Bob Withers, Director of Public Sector, New Relic

To what extent do agencies have an accurate gauge of the performance and security of their applications and systems? As enterprise IT environments have grown more complex, such visibility has become more elusive. Agencies might have basic monitoring capabilities, which enable them to track specific metrics. But monitoring is not enough.

What they need is the ability to observe the performance of their systems from end to end in real time – and when a problem arises, to identify its source. That is the purpose of an observability platform.

To learn more about this capability, GovLoop spoke with Bob Withers, Director of Public Sector at New Relic, which provides a cloud-based programmable observability platform. He identified three key ways in which an observability platform can help agencies improve their IT operations and services.

Minimizing the Costs and Risks of Cloud Migration

When agencies move applications to the cloud, they generally expect to reduce the cost of operations and improve performance. The problem is that they often do not have any clear measure of whether that bears out.

An observability platform provides the ability to get a detailed picture of cost and performance before, during and after a cloud migration. If problems arise, the platform makes it possible to trace those problems to their root. This is especially important because many systems involve hundreds of components, all of which factor into the performance and cost-effectiveness of that system.

Such insights also can help agencies determine upfront whether it makes sense to move an application to the cloud or keep it on premises. "You want to make informed decisions," Withers said.

Improve the Citizen Experience

The complexity of operations also makes it difficult for agencies to gauge the user experience. End-user or citizen services often involve multiple applications and systems, each of which must be factored into an overall picture of the end-user experience.

For example, in the case of a citizen-facing service, performance depends on such variables as the quality of connection in the end users' area, the browser they are using and their operating system, all of which must be factored into application performance.

New Relic has adopted a standard scoring system, called Apdex, that factors in a wide range of dependencies to assess both application performance and the overall user experience.

Enforcing Security Controls

Any discussion of a cloud-based system must begin with the Federal Risk and Authorization Management Program (FedRAMP), a government-wide program that provides a standardized approach to security.

New Relic has received FedRAMP authorization at a moderate impact level. Unlike many vendors who put specific releases through the FedRAMP process, New Relic has just one version of its software-as-a-service offering, which means all customers, federal or not, get the benefits of FedRAMP security.

"I like to say that New Relic is FedRAMP compliant, not just our application," Withers said. "We are absolutely all in."

Additionally, all the performance data gathered by the observability platform can be fed into an agency's cyber solution, providing new insights into agency operations.

TIC Gets Agile

An interview with Sean Connelly, TIC Program Manager, CISA

The TIC policy is a work in progress — and that's not a flaw, it's a strategy. When it first announced the TIC initiative, OMB said that its goal was to reduce the federal government's number of connections to the internet to 50. But that was before anyone realized the extent to which cloud computing would alter how agencies manage IT. With the release of TIC 3.0 draft guidance in December 2019, the TIC program office is looking to ensure that the policy can evolve as agency strategies evolve.

To learn more about this, GovLoop interviewed Sean Connelly, TIC Program Manager at CISA.

New Use Cases

One of the most interesting aspects of TIC 3.0 is the role of use cases, Connelly said. The goal of a use case is to describe how agencies can provide a secure connection when traffic is not flowing through a physical TIC access point. For example, one of the first new use cases deals with remote offices, while forthcoming cases will address telework, various cloud services and zero trust security. The TIC Use Case documentation will outline which alternative security controls, such as endpoint and user-based protections, are required.

"With TIC 1.0 and TIC 2.0, there was just one reference architecture, and that was the way the agencies were able to meet the intent of the TIC policy from OMB. But now with TIC 3.0, we have the flexibility to provide alternative architectures for agencies to use if they want, rather than just the traditional TIC access point as the primary solution."

However, Connelly notes that although there clearly is a need for these alternative architectures, they do not necessarily supersede traditional TIC.

"We've talked to a lot of agencies that still look at traditional TIC as their access point, so that's still a very viable solution for agencies to use. I talked to some agencies who said they're all in on zero trust or all in on this alternative use case. That's fair if it works for them, but also some agencies are perfectly comfortable using that traditional TIC access point."

Defining Trust Zones

As with FedRAMP, CDM and other security initiatives, TIC is changing to make it easier for agencies to deal with the demise of the network perimeter as they adopt cloud, mobility and related technologies.

In the past, the network perimeter defined a clear boundary where security controls were applied. Today's complex IT environment means agencies need a more nuanced approach, with different parts of their environment requiring different levels of security. TIC 3.0 addresses this by supporting the definition of multiple "trust zones" within the environment.

"The trust zones are abstracts — they're notional, they're conceptual. They're for whatever the agency's trying to secure at that time. When you look now at the trust zone, a lot of agencies consider their networks to be the trust zone, which is certainly possible. But, later on, we'll start to see that the network is more abstracted away, and the trust zones may become more the endpoints, or the edge. Even as you move more toward zero trust, that network is abstracted away. It's more toward the application and the user or identity on top of it. I think that's where you'll see the trust zone starting to move also. But right now, it's just a gradual learning process of how we're going to use this going forward."

A Collaborative Process

To keep TIC grounded in reality, the TIC program office works closely with agencies to select and define use cases.

Once the office selects a use case — a process the Federal Chief Information Security Officer Council TIC Subcommittee drives — it recruits agencies to conduct pilots and provide lessons learned that shape the final use case. The TIC program office works closely with agencies throughout the process.

"The pilots are dependent on the agency's time frame, and they often have some external dependencies. Some pilots we've been able to complete in a few months, while other pilots have taken over a year. But we understand the challenges. Some of the challenges are acquisition-related, some of the challenges could be vendor-related. And some challenges can just be getting everyone inside the agency to understand what we're doing with the pilot itself. So, there are a number of things that may come up and delay the pilot. But in the end, we work with the agencies almost on a weekly basis."

As part of the collaborative process, the program office and other stakeholders are always looking out for new potential use cases, Connelly said.

"We've heard a lot of interest in [the] Internet of Things. Let's say an agency has sensors out on the internet. How does that sensor telemetry come back to the agency? Partner networks represent another potential use case. A lot of agencies connect to banks or to research and development at universities. What are the best ways to meet the intent of TIC while connecting to those environments? The agencies usually have some type of relationship with [those organizations]; they can't fully trust those networks. We might also do some type of use case with GSA and their Enterprise Infrastructure Solutions vehicle."

Clearly, with TIC 3.0, change is now the norm.

Transform Federal Government IT

Speed? Agility? Better economics? Yes.
Get the hybrid cloud that delivers it all.
With VMware Cloud Foundation™,
be ready for any.

Learn more at
vmware.com/go/federal

vmware®

REALIZE WHAT'S POSSIBLE.™

INDUSTRY SPOTLIGHT

The Cloud Era Requires Cloud-Ready Cyber Policies

An interview with Ethan Palmer, Senior Pre-Sales Solutions Engineer, VMware GEH Team, Carahsoft

As federal agencies accelerate their effort to move data, applications and services to the cloud, they often run into an obstacle: Their existing cyber policies and processes were developed with a physical IT infrastructure in mind, not the virtual infrastructure that is the basis of so many modern solutions.

TIC 3.0, FedRAMP and other evolving policies are geared toward helping agencies make this move to the cloud. But "in order for these new policies to pave the way for datacenter modernization, you have to make sure that the old policies and legacy datacenters can align and be flexible when it comes to adopting these new technologies," said Ethan Palmer, Senior Pre-Sales Solutions Engineer, VMware GEH Team at Carahsoft.

In an interview with GovLoop, Palmer highlighted four policies that agencies should consider.

Zero Trust Architecture

Conceptually speaking, zero trust involves shifting from a blacklist mindset, which depends on identifying and blocking malicious or suspicious activity, to a whitelist mindset, in which users or systems must be explicitly approved before accessing a network resource.

Practically speaking, it requires a defense-in-depth approach in which firewalls are not just at the perimeter, but throughout the enterprise. Better yet, agencies can deploy security controls in the virtual layer, which makes it possible to monitor network activity and enforce security policies at the application layer, Palmer said.

DMZ Anywhere

A "demilitarized zone," or DMZ, is a place on a network where an organization can provide access to a limited set of resources or services without exposing their internal systems. In a traditional network, the DMZ has its own hardware stack, with physical firewall devices protecting the network perimeter.

In today's virtualized enterprises, however, agencies can set up DMZs anywhere within the enterprise by using logical firewalls at the software level – which eliminates the need for a dedicated hardware stack, reduces the number of physical firewalls that an agency must buy and provides much more granular security control, Palmer said.

Secure Remote Offices

While data center consolidation is a priority, agencies know they will always have remote offices that need local compute power. In a traditional IT environment, that requires a local hardware stack and complex network infrastructure, with all traffic backhauled through security controls back at the data center.

A software-defined wide area network (SD-WAN) simplifies this environment by enabling agencies to extend security controls to the edge and to optimize network traffic between a remote office and the primary data center. This approach provides those offices with optimal connectivity to resources both in the central data center and in the cloud.

Secure End Users

Increasingly, agencies recognize they need to think about security at the level of individual end-users wherever they are working – and they need the ability to enforce those policies automatically.

A secure end-user model requires a combination of technologies and policies. First, device management ensures that the end-user's device complies with security policies around authentication, encryption and other security measures. Second, the practice of least privilege management applies identity and access management controls to ensure that end-users can access only those resources that they need to do their jobs.

Carahsoft and VMware provide solutions that enable agencies to build a modern cloud-based infrastructure that enforces security policies throughout the enterprise. By adopting VMware's NSX, agencies can achieve zero-trust and DMZ anywhere. Also, they can extend their network and security to the edge with VMware SD-WAN by VeloCloud. Finally, they can secure endpoint devices and manage users with VMware WorkspaceONE and VMware Carbon Black's next generation anti-virus solution.

CDM Keeps Eye on Shifting Cyber Requirements

An interview with Kevin Cox, CDM Program Manager, DHS

DHS, in collaboration with GSA, launched CDM in 2012 to help the federal government take a more consistent approach to cybersecurity and to provide individual agencies and the federal government as a whole with a better understanding of the security of their networks.

DHS generally describes CDM as helping agencies answer four questions:

- What assets are on the network?
- Who is on the network?
- What is happening on the network?
- And how is the data protected?

Early on, as a key part of the strategy, agencies deployed network sensors that feed operational dashboards that provide a real-time status check on the enterprise's security. Now DHS and the agencies are looking at how to roll that data up into a federal-level dashboard.

To learn more about developments with the CDM program, GovLoop spoke with Kevin Cox, CDM Program Manager at DHS.

Status Check

Cox said now that many of the tools are in place at agencies across government, the focus is on "operationalizing" that data, both at the individual agency and at the federal levels.

"We need to make sure that, No. 1, the data that's getting reported up is of high quality — that we can match up data coming off a sensor to the data that's in the dashboard. And that, No. 2, once we confirm the quality of the data, that we then have the mechanisms to use that data to help agencies better manage their risk and to help the federal government get better visibility across the entire federal landscape, so that they know where they need to prioritize actions in regards to cybersecurity risk management."

DHS is working steadily toward that goal of cross-government visibility. Some of the most important gains to date have been helping agencies address basic but critical cyber hygiene issues, Cox said.

"The biggest benefit at this stage is getting the CDM technologies — the sensors — out to the agency networks, to help the agencies better understand what their asset environment looks like, understanding what's connected and how well it is patched and configured. We know in talking with the agencies that they've used the CDM tools to identify where critical vulnerabilities are, and to work to get them patched, and to help identify where there are misconfigurations and get those fixed as well.… The sensors also help them to understand who all their credentialed users are, as well as their privileged users."

An Evolving Program

Cox talks about current CDM efforts in terms of "maturing" the program, helping agencies learn how to extend CDM capabilities to address new challenges. One primary example is the cloud.

"If CDM started with a focus of the agency on-premises environment, we now want to help agencies as they move out to the cloud — help them get a better understanding of where their data is, how it's protected, who has access to it. And as agencies do more with mobility and mobile devices, we want to make sure they understand where their mobile assets are and what the threat environment looks like both for mobile and cloud. So, that's where we want to continue to mature as well: helping agencies get the right capabilities in place, get the right visibility, to ensure that wherever their data might be — whether it be on prem, in the cloud or on a mobile device — that it's properly protected. That's the second-level maturity we're working with the agencies on."

Other focus areas include using more automation to improve the overall cybersecurity risk management process and shifting from point-in-time to ongoing cyber assessments. DHS and GSA are using DEFEND acquisition to support innovative efforts.

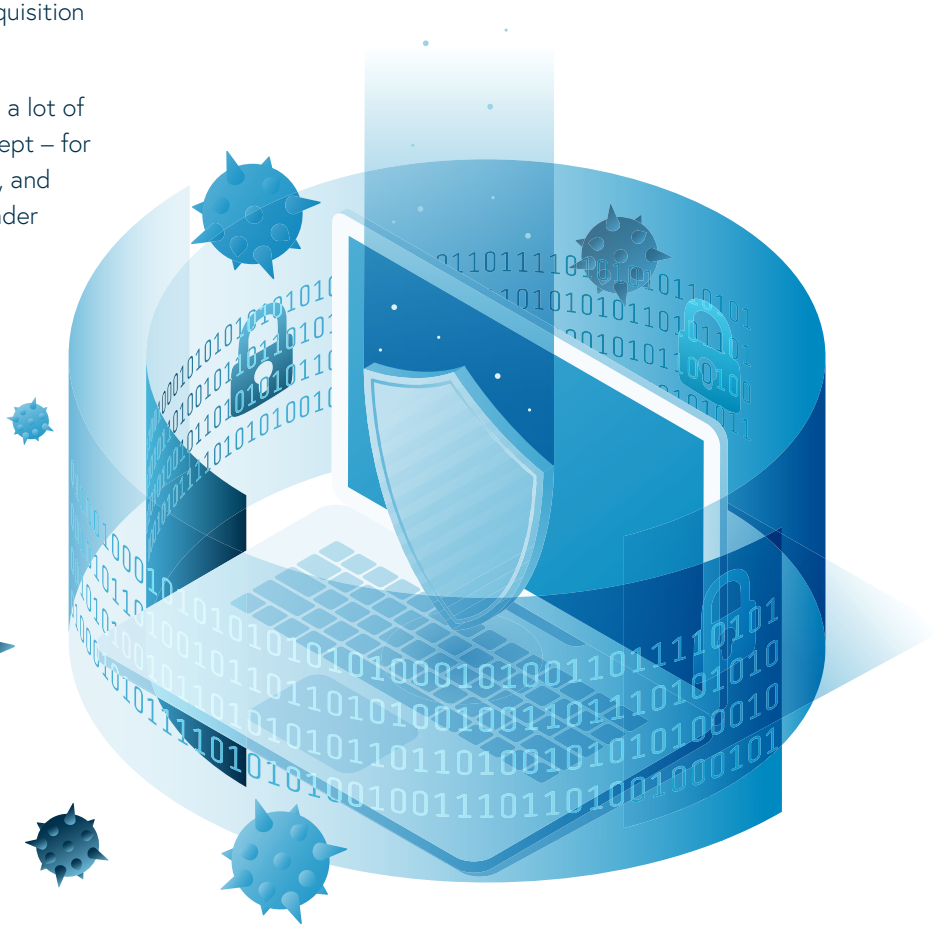
"With our new DEFEND task orders, we've created a lot of flexibility to be able to do different proofs of concept – for example, to try different ways to secure the cloud, and then use those lessons learned to feed into a broader approach, a broader solution set for the federal government. We've been real happy with that ability to try a particular approach at one agency, rather than all agencies, and then learn from the lessons and then expand it out from there for all the agencies."

"What we want to do is work together to identify those solutions that help agencies get better visibility overall into where there is risk in their environment"

The Big Picture

CDM, of course, is just one of several federal-wide programs that aims to raise the cyber baseline in government. With that in mind, the CDM program office is working closely to ensure that CDM aligns with other programs. That includes the National Cybersecurity Protection System, which is designed to provide advanced capabilities in intrusion detection and prevention, analytics, and cyber information sharing across government (known as the EINSTEIN set of capabilities); the TIC initiative spearheaded by OMB; and GSA's FedRAMP program.

"What we want to do is work together to identify those solutions that help agencies get better visibility overall into where there is risk in their environment — where threat actors might be trying to get in, whether that's through the traditional perimeter or in a cloud somewhere. Where some of those different program management offices have different specific needs, we look at where CDM can help to align [with them] and make sure that the agencies are getting a full solution to protect their environments and their critical data."




Zero Trust Security
Because People are the New Perimeter
The traditional four walls that protected an organization's data no longer exist: More people are accessing more resources, and from more locations, than ever before. Learn how government agencies can utilize Okta as the foundation for a successful Zero Trust program now, and in the future.
Learn More at okta.com/ZeroTrustModel
okta
Gartner & Forrester Leader
FedRAMP Authorized
CAC/PIV Support

INDUSTRY SPOTLIGHT

Identity Emerges as Key Piece of Modern Cybersecurity

An interview with Michelle Tuggle, Principal Security Analyst, Security & Compliance, Okta

Identity and access management is essential to modern cybersecurity. As agencies transform their IT environments through the adoption of cloud solutions, they need to ensure they can easily manage which users have access to which applications and data. Without that ability, transformation simply creates too many vulnerabilities.

The challenge is that cloud solutions extend applications and data outside the traditional network perimeter and security controls. The more cloud solutions that agencies adopt, the more challenging it is to manage that environment.

"As the cloud grows, so grows the need for pristine identity and access management," said Michelle Tuggle, Principal Security Analyst, Security and Compliance at Okta, which provides cloud-based identity solutions. GovLoop recently spoke with Tuggle to discuss the role of identity and access management in federal agencies.

A commitment to privacy, security

Not only does Okta help agencies securely adopt cloud solutions, it also provides its solution through the cloud. As Tuggle said, "Okta was born in the cloud." From the beginning, the company has made privacy and security its top priorities.

From a privacy perspective, Okta adheres to three fundamental principles:

- Customers own their data.
- Okta only uses their data to provide the service.
- Okta keeps its customers' data safe and secure.

Okta employees can access customer data in one of two ways. First, customer support uses custom tooling that is protected by the Okta Identity System, with access limited to employees who require access to do their jobs and enforced using FedRAMP-compliant authentication.

Second, Okta's operations team accesses customer data via a Secure Socket Layer virtual private network, with team members using an Okta-managed certificate placed on an Okta-managed endpoint, plus a physically separate FIPS 140-2 Level 1 validated hardware multifactor authentication token.

As a foundation of its security strategy, the company has made a firm commitment to the FedRAMP program.

Okta's cloud platform is currently classified as a FedRAMP Moderate or Impact Level 2 (IL2), and is working towards getting its FedRAMP M+ classification (IL4). In the near future, the company expects to move to FedRAMP High (IL5).

Earlier this year, Okta was selected to work with the FedRAMP Joint Authorization Board (JAB) for a Provisional Authority to Operate (P-ATO) as part of the FedRAMP Connect initiative. The JAB prioritizes cloud service offerings based on government-wide demand to help meet government-wide mission needs.

Zero trust requires collaboration

Going forward, Okta looks forward to supporting agencies as they move to a zero trust architecture.

As part of zero trust, an agency applies security measures at the level of individual applications, data or systems, and verifies the identity and permission level of every end user or device requesting access. Obviously, identity is key to zero trust, but it is only part of the solution.

"Okta is focused on being a collaborative partner," Tuggle said. "We know that from a zero trust perspective we can't do this alone. It's going to take several partners and several IT sections to come together to create some of these zero trust environments."

FedRAMP Responds to Agency, Industry Pain Points

An interview with Ashley Mahan, FedRAMP Director, GSA

Like TIC and CDM, FedRAMP continues to evolve to meet evolving security requirements. GSA launched FedRAMP in 2011 to provide a baseline for cloud security at a time when the cloud market was beginning to boom. Now, with agencies accelerating their adoption of the cloud — and industry accelerating their development of cloud solutions — the FedRAMP program office is taking steps to improve the efficiency of its authorization process.

To learn more, GovLoop conducted an email interview with Ashley Mahan, FedRAMP Director.

This interview has been edited for clarity and length.

GOVLOOP: At this point, how do you define the FedRAMP value proposition, and how has it evolved since FedRAMP's inception?

MAHAN: FedRAMP's mission is to promote the adoption of secure cloud services across the U.S. government by providing a standardized approach to security and risk assessment. The FedRAMP core value proposition is championing a common set of security requirements and a standard authorization framework that is recognized by all agencies. This approach uses a "do once, use many times" framework that saves on the cost, time and staff required to conduct redundant agency security assessments, and makes it easier for cloud service providers and small companies to meet security requirements for multiple agencies. FedRAMP:

- Reduces duplicative efforts, inconsistencies and cost inefficiencies associated with the current security authorization process.
- Establishes a public/private partnership to promote innovation and the advancement of more secure information technologies.
- Enables the federal government to accelerate the adoption of cloud computing by creating transparent standards and processes for security authorizations and allowing agencies to leverage security authorizations on a governmentwide scale.

How does FedRAMP fit into broader issues around IT modernization and transformation?

FedRAMP is the bridge connecting cutting-edge industry innovation to government IT modernization and transformation initiatives. The program drives secure cloud adoption by providing a standardized security framework for cloud security, allowing agencies to take full advantage of modern cloud solutions.

How might FedRAMP fit into the concept of zero trust architecture?

FedRAMP encourages and embraces new technologies and ways of thinking about security, including zero trust architecture (ZTA). The foundation of the FedRAMP baseline is the NIST Risk Management Framework and applies in a ZTA. The zero trust concept of micro-perimeters is inherent in the Risk Management Framework and the security controls are generally flexible enough to allow implementation of various security architectures, including ZTA.

How are you looking to increase participation in FedRAMP?

We have made a deliberate push over the past few years to augment our support and training to agencies as they serve an integral role within the program and authorization process. FedRAMP will continue to scale through

agencies, and we want to enable the federal government to accelerate their adoption of cloud computing by maximizing reuse and diminishing authorization timelines.

As we look ahead, we are excited to establish a volunteer FedRAMP Agency Liaison Program among the agency community. The goals of creating this program are to increase collaboration, promote a unified understanding of FedRAMP, institute formal feedback channels, enhance visibility into FedRAMP strategic initiatives and create an incredible team of FedRAMP experts across government.

How will FedRAMP evolve in the next year or so?

Our attention is focused on four areas over the next year: automation, growing the FedRAMP Marketplace, simplifying the program and providing more learning opportunities for the FedRAMP community. Through these initiatives, our goals are to see an increase in government entities participating in the program, a reduction in authorization timelines, and have more cloud products authorized and reused across government.

By the end of FY 2020, we hope to have the entire security package within the Open Security Control Assessment Language (see sidebar). Draft versions of all the FedRAMP baselines and system security plan have been released for public comment at the end of 2019. The team is working on the Security Assessment Plan and Security Assessment Report and will release draft versions in late spring.

Additionally, to better align with real-world cyber risk and volatility, the FedRAMP program office is working with DHS in using the .govCAR methodology to score controls within the FedRAMP moderate baseline against the National Security Agency/Central Security Service Technical Cyber Threat Framework. This research could fuel a threat-based approach to authorizations, which enables agencies to make risk-based decisions by focusing on security controls that protect against known and potential significant/consequential threats.

We are ramping up on training and outreach activities for industry, small businesses and agencies this spring. Our next Agency Information System Security Officer Training Day is scheduled for June 30. If you are interested in attending, please email info@fedramp.gov.

Automating the Authorization Process

The FedRAMP program office has been working closely with NIST and industry to develop the Open Security Controls Assessment Language (OSCAL). OSCAL provides a way of describing security controls in a machine-readable format. That paves the way for automating the process of assessing the security controls of systems going through the FedRAMP authorization process.

Here are some of the anticipated benefits of OSCAL:

- Cloud service providers will be able to create their system security plans more rapidly and accurately, validating much of their content before submitting it to the government for review.
- Third-Party Assessment Organizations will be able to automate the planning, execution and reporting of cloud assessment activities.
- Agencies will be able to expedite their reviews of the FedRAMP security authorization packages.

"FedRAMP is the bridge connecting cutting-edge industry innovation to government IT modernization and transformation initiatives."

INDUSTRY SPOTLIGHT

Evolving Cyber Policies Clear Way for Cloud Adoption

An interview with John Amorosi, Senior Solutions Architect for Federal Civilian Agencies, McAfee

The federal government's sudden, widespread transition to a remote work environment has highlighted the importance of its decision to make policy decisions that remove barriers to cloud adoption.

In particular, the Trusted Internet Connection (TIC) 3.0 initiative has opened the floodgates for increased cloud utilization in a more efficient and holistic manner, said John Amorosi, Senior Solutions Architect for Federal Civilian Agencies with McAfee, the device-to-cloud cybersecurity company.

The changes have greatly expanded an agency's ability to embrace cloud technology without degrading performance – while still applying appropriate security controls and reducing end-user friction. DHS has indicated they are transitioning the TIC program to a more descriptive, not prescriptive methodology, recognizing that there's no one-size-fits-all approach to securing agency data.

"The new expanded and increased flexibility will empower agencies to protect agency data, secure and monitor cloud services, and protect remote users regardless of device and location," Amorosi said.

In the same vein, the most recent iteration of the Continuous Diagnostics and Mitigation (CDM) program extends the framework to cloud and mobile devices.

CDM has been a catalyst for agencies to gain greater visibility of the assets in their environment while improving their cybersecurity posture, including both Network Security and Data Protection. Agencies should look to leverage the synergies between the two programs by enhancing their enterprise architecture and embracing the cloud, said Amorosi.

Following a rationalization of their existing toolsets and developing a strategy, agencies can accomplish this by drafting a Request for Service (RFS) to introduce new CDM capabilities that fully address the requirements, goals and efficiencies of both programs while improving the end-user experience.

A New Architecture

With TIC 3.0 and CDM, agencies are no longer required to put all security controls within the network perimeter but instead can extend security to data, devices and applications at the edge. With that architecture, end-users can access cloud services directly, rather than having all network traffic routed back to the agency's security stack in the data center. This approach will provide some much-needed boosts in network and application performance.

That is not to say that all data or applications are going to the cloud. Instead, agencies need to develop a cybersecurity framework that protects data and applications whether they are in the cloud or within the network perimeter, Amorosi said.

McAfee recently released what it calls the Unified Cloud Edge (UCE).

UCE is built around three pillars:

- McAfee Cloud Access Security Broker, which offers visibility and control over data across different cloud environments
- McAfee Web Gateway, a cloud-native service that protects against web-based threats
- McAfee Data Loss Prevention, which safeguards sensitive data on devices, in transit to the cloud and within the cloud.

"Our goal is to provide agencies with technologies that serve as Policy Enforcement Points (PEP) that they can employ to expand cloud adoption and fully support TIC 3.0 use cases, as well as support CDM goals and improve the security posture of the enterprise," Amorosi said.

Best Practices in Federal Cybersecurity

A Security Capabilities Punch List

The draft TIC 3.0 guidance identifies "universal security capabilities" that might be applied across an enterprise and that can be mapped against the NIST Cybersecurity Framework. Here is a sampling:

- ☑ **Backup and Recovery**
  Keeping copies of configuration and data, as needed, to allow for the quick restoration of service in the event of malicious incidents, system failures or corruption.
- ☑ **Central Log Management with Analysis**
  Storing telemetry data needed to discover and respond to malicious activity in a manner that facilitates security analysis and data fusion.
- ☑ **Configuration Management**
  Implementing a formal plan for documenting, and managing changes to the environment and monitoring for deviations.
- ☑ **Inventory**
  Developing, documenting and maintaining a current inventory of all systems, networks, and components so that only authorized devices are given access and unauthorized and unmanaged devices are found and prevented from gaining access.
- ☑ **Least Privilege**
  Designing the security architecture such that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.
- ☑ **Strong Authentication**
  Verifying the identity of users, devices or other entities through rigorous means (e.g., multifactor authentication) before granting access.
- ☑ **Enterprise Threat Intelligence**
  Obtaining threat intelligence from private and government sources and implementing mitigations for the identified risks.
- ☑ **Situational Awareness**
  Maintaining effective awareness, both current and historical, across all components.
- ☑ **Dynamic Threat Discovery**
  Using dynamic approaches (e.g., heuristics, baselining, etc.) to discover new malicious activity.
- ☑ **Integrated Desktop, Mobile and Remote Policies**
  Defining polices such that they apply to a given agency entity no matter its location.

Find the full list in the TIC 3.0 Security Capabilities Handbook.

TIC 3.0: The Hallmarks of a Good Pilot Project

As noted earlier, TIC 3.0 pilot projects are essential to the development of TIC use cases. Once a use case has been proposed, the TIC program office will look to agencies to run pilots and develop best practices and lessons learned to shape the final use case.

According to CISA, a pilot should meet the following criteria:

- Address technology that can be used by the broader federal government
- Identify applicable security capabilities to secure their environments
- Explain how the applicable security capabilities requirements are met
- Follow a defined and structured timeline
- Be carefully considered and planned
- Be supported by agency leaders

To learn more about pilot projects, check out the TIC 3.0 Pilot Process Handbook.

Managing Multi-Agency Continuous Monitoring

When multiple agencies use a common cloud service, continuous monitoring can get complex because of the shared responsibility to manage the cloud service provider's Authorization to Operate. To make it easier, the FedRAMP program office recommends these best practices:

1. **Establish a collaboration group of agencies leveraging the service.** The group should meet regularly (e.g., monthly or quarterly) with the cloud service provider (CSP). They should establish a standard agenda and formalize communications channels for sharing questions, meeting minutes and decision points across group members.
2. **Standardize the continuous monitoring requirements that the CSP must meet.** This will streamline the review and approval of a cloud service security posture. As part of this, the group should develop a standard report that summarizes a CSP's continuous monitoring evidence, and that evidence should be presented using a standard nomenclature and taxonomy.
3. **Define a governance protocol for the evaluation, approval and review of significant changes proposed by the CSP.** That protocol should include defining a "lowest common denominator" for the qualification of a proposed change. The key question to ask is: What does each participating agency consider to be a significant change? The CSP should describe the impact of a proposed change in terms of agency-specific use cases.

Source: FedRAMP

"As federal agencies increasingly use cloud computing to perform their missions, the implementation of effective information security controls becomes more important. The effective implementation of a standardized process for securing cloud environments could reduce risks to agency systems and information maintained on an agency's behalf."

- A 2019 GAO report on cloud computing security

Get the Most Out of Least Privilege

One of the central tenets of modern cybersecurity is the concept managing the specific systems and even facilities that users are authorized to access. The goal is "least privilege" — that is, users should be able to access only those resources they specifically need to do their jobs. With this in mind, the CDM program offers a Manage Privileges and Accounts (PRIV) security capability. Here is a short FAQ:

What security results should we be able to achieve by implementing PRIV?

The PRIV security capability will help ensure that authorizations and accounts do not exceed the privileges required by a user's attributes (or specific needs to meet his or her job duties).

What type of security issues are addressed by the PRIV security capability?

In a typical agency, privileges are assigned locally based on requests for access. Over time, as jobs and missions change, more privileges are granted to individuals and few are rarely (if ever) removed. The effects of such aggregated privileges across an organization can represent great risk.

What can I do to reduce my exposure to attacks exploiting poor privilege management?

Users are given certain privileges to perform work on systems. These privileges are often denoted by roles, also known as attributes, or security groups to which a user is assigned. To reduce exposure to attacks, an agency must define what access user roles can have. This includes continuously monitoring user accounts to ensure each account matches the user's duties and does not provide excess privileges. Accounts that are no longer in use (e.g., after an employee leaves a position or after test accounts perform a network assessment) should be disabled or deleted, since they are often targeted by attackers to gain unauthorized access.

Read the full FAQ and access other resources here.

Gigamon®

Network Visibility and Analytics for Government Innovators

Gigamon is the first company to deliver a unified visibility and analytics architecture for network agility, security and cost management across your hybrid infrastructure.

READY TO LEARN MORE, VISIT

gigamon.com/government

INDUSTRY SPOTLIGHT

Intelligent Network Visibility Serves as Security Force Multiplier

An interview with Dennis Reilly, Vice President, Federal, Gigamon

Any discussion about improving the security of the federal IT enterprise sooner or later comes around to the topic of network visibility.

The concept of network visibility – the idea that an agency should have a clear picture of all data-in-transit moving across the enterprise – is not new. But it has taken on new importance as agencies have extended applications and data from the traditional IT infrastructure to virtual and cloud infrastructures. If an agency lacks visibility across all three environments, they leave themselves vulnerable.

Both the TIC and CDM initiatives have evolved to help agencies strengthen their cyber posture as they adopt cloud, mobility and other technologies as part of their IT modernization efforts. But the importance of securing this extended enterprise has been driven home more recently by the COVID-19 pandemic. As the virus spread, many employees ended up working from home.

To learn more about how agencies can improve network visibility in this environment, GovLoop spoke with Dennis Reilly, Vice President for Federal at Gigamon, which provides network visibility and analytics for data-in-transit.

One of the primary challenges in a remote work environment is the volume of traffic that needs to be inspected. Many agencies provide employees with connectivity through a virtual private network (VPN) which routes all traffic through the on-premises network. That doubles the workload for the security infrastructure, since it will end up inspecting network packets as they come onto the network and again as they go out.

Rather than just increasing that infrastructure, agencies should look for a solution that can strip out those duplicate packets, cutting the workload in half, Reilly said. They can further reduce the workload by inspecting only relevant traffic, such as email for a phishing threat, as opposed to video or voice-over-IP, which don't pose a significant risk. One of Gigamon's DoD customers did just that recently.

The goal is not just to inspect individual network packets but to monitor traffic patterns for anomalies. For example, is data being moved around the network, possibly in preparation for exfiltration? Is an end user or system communicating with a server that they don't normally access?

By providing agencies with such intelligence, companies like Gigamon serve as a "force multiplier," Reilly said.

Beyond the current crisis, network visibility is essential to achieving the aims of the CDM program. While much of the initial work on CDM was focused on identifying the devices and users on the network, the more advanced capabilities involve seeing all traffic that's traversing the network.

This is especially important in the TIC 3.0 environment, which no longer requires all network traffic to be routed back to the enterprise network. The challenge is ensuring that agencies don't lose visibility into that traffic.

"If you can't see the traffic that's traversing the network – whether that's a physical network, a virtual environment, or even out to the cloud – you can't secure it," Reilly said.

In short, when it comes to network visibility, a blind spot is vulnerability. Through CDM, Gigamon helps agencies to eliminate those blind spots, he said.

TIC 3.0 Starter Kit

Foundational Definitions and Concepts for Tackling TIC 3.0

(Source: The TIC 3.0 Security Capabilities Handbook)

TIC Terms and Concepts

Here are the definitions of key TIC terms. A full glossary is provided in the TIC 3.0 Program Guidebook.

- **Boundary:** A notional concept that describes the perimeter of a zone (e.g., mobile device services, general support system [GSS], Software-as-a-Service [SaaS], agency, etc.) within a network architecture.
- **Hybrid TIC Model:** An alternative approach to implementing TIC services that blends the use of agency hosted and managed TIC access providers (TICAP) and MTIPS solutions.
- **Managed Trusted Internet Protocol Services (MTIPS):** Services under GSA's Enterprise Infrastructure Solutions (EIS) contract vehicle that provide TIC solutions to government clients as a managed security service.
- **Management Entity (MGMT):** A notional concept of an entity that oversees and controls the protections for data.
- **Policy Enforcement Point (PEP):** A security device, tool, function or application that enforces security policies through technical capabilities.
- **Security Capability:** Used to articulate security best practices and provide appropriate mission and business protections. Security capabilities are typically defined by bringing together a specific set of safeguards and countermeasures and implemented by technical means.
- **TIC Access Point:** The physical location where a federal civilian agency consolidates its external connections and has security controls in place to secure and monitor the connections.
- **Trust Zone:** A discrete computing environment designated for information processing, storage and/or transmission that dictates the level of security necessary to protect the traffic transiting in and out of a zone and/or the information within the zone.

What Makes a Viable Security Capability?

The TIC 3.0 Security Capabilities Handbook highlights capabilities that can address requirements created by modern and emerging technologies. DHS said that its choice of capabilities was guided by four criteria:

1. **Technology Maturity:** Is the underlying technology mature enough to support the adoption of the capability?
2. **Sensor Positioning:** Can the capability be positioned to effectively measure performance and security within a network or environment?
3. **Policy Enforcement Point (PEP) Deployment:** Can the capability be deployed at a PEP within a given TIC implementation scenario?
4. **Scoped to TIC Initiative:** Does the capability's purpose fall within the scope of TIC (i.e., baseline network security, consolidation of trusted connections, address TIC security objectives)?

As modern architectures become both more complex and diverse, TIC 3.0 accommodates a wide variety of scenarios, focusing on cloud, mobility and encryption. TIC 3.0 guidance intentionally has a different tone and level of detail when compared to earlier iterations to accommodate this wider variety of environments.

- TIC 3.0 Program Guidebook

TIC 3.0 Security Objectives

While the original TIC policy was intended to limit an agency's threat surface, TIC 3.0 is focused on limiting "the potential impact of a cybersecurity event," according to the Security Capabilities Handbook. In this spirit, DHS defines six basic security objectives:

1. **Manage Traffic:** Observe, validate and filter data connections to align with authorized activities; least privilege and default deny.
2. **Protect Traffic Confidentiality:** Ensure only authorized parties can discern the contents of data in transit, sender and receiver identification and enforcement.
3. **Protect Traffic Integrity:** Prevent alteration of data in transit; detect altered data in transit.
4. **Ensure Service Resiliency:** Promote resilient application and security services for continuous operation as the technology and threat landscape evolve.
5. **Ensure Effective Response:** Promote timely reaction and adapt future response to discovered threats; policies defined and implemented; simplified adoption of new countermeasures.
6. **Use Case Applicability:** Does the capability apply to one or more networking scenarios (such as those outlined in TIC Use Cases)?

Policy Enforcement Point Capabilities

DHS defines PEPs as network-level capabilities that inform technical implementation for relevant use cases. They divide PEPs into eight categories, each with its own set of capabilities. Here is a sampling of those capabilities:

- **Files:** Anti-malware, content disarm and reconstruction, detonation chamber.
- **Email:** Anti-phishing protections, anti-spam protections, authenticated receive chain, data loss prevention, encryption, malicious URL protection.
- **Web:** Break and inspect, active content mitigation, certificate blacklisting, content filtering, authenticated proxy, malicious content filtering.
- **Networking:** Network access controls, IP blacklisting, host containment, network segmentation and microsegmentation.
- **Resiliency:** Distributed Denial of Service protections, elastic expansion, regional service delivery.
- **Domain Name System:** DNS blackholing, Domain Name System Security Extensions (DNSSEC) for agency clients, DNSSEC for agency domains.
- **Intrusion Detection:** Endpoint detection and response, intrusion protection systems, adaptive access controls, deception platforms, certificate transparency log monitoring.
- **Enterprise:** Security and Orchestration, Automation and Response (SOAR), shadow IT detection, virtual private networks.

proofpoint®

Anyone can be a VAP

VERY ATTACKED PERSON

Protection starts with people.

Learn how Proofpoint can help you protect your remote workforce against today's biggest cyber threats at www.proofpoint.com.

INDUSTRY SPOTLIGHT

Why a People-Centric Approach to Security Has Become a Necessity

An interview with Bruce Brody, Resident Chief Information Security Officer (CISO), Federal Practice, Proofpoint

For years, cybersecurity experts have said that the weakest link in an agency's cyber defense is not a system but a human – the employee who clicks on a link in an email that introduces malware onto the network. Nonetheless, most organizations continue to think about security strictly as a technology issue.

A technology-centric approach to cybersecurity is essential, but not sufficient. Think about it from the attacker's perspective. What is easier: identifying and exploiting the vulnerability of a network, or tricking a user into clicking on a link opening an attachment? The nation's recent history of data breaches, many of which began with phishing attacks, suggests that agencies need to take a people-centric approach as well.

To learn more about the human dimension of security, GovLoop spoke with cyber experts at Proofpoint, which offers an integrated suite of FedRAMP-authorized cloud-based, people-centric solutions.

The key to people-centric security is to identify those individuals within the organization that are at the highest risk of being targeted. Proofpoint calls those individuals "Very Attacked Persons" (VAPs).

"Malicious actors have become very adept at using org charts, social media and other tools to identify people with desirable network privileges and engineer highly targeted attacks," said Bruce Brody, Resident Chief Information Security Officer (CISO) for Proofpoint's Federal practice. Brody also served as CISO at the Department of Veterans Affairs and the Department of Energy.

A VAP is not necessarily someone high on the org chart. Instead, it might be a lower-level employee whose responsibilities require them to have access to a wide range of network resources. To identify VAPS, Proofpoint developed an Attack Index that reflects the risk of a given threat, or set of threats, to a given individual.

The Attack Index assigns every threat a score of 0-1000, based on three key components:

- Actor type, which considers the criminal's level of sophistication. Does it appear to be a state-sponsored actor or typical small crime actor?
- Targeting type, which looks at the degree of targeting involved with the threat. Is it focused on a particular user, organization or sector, or is it a general-purpose attack with no particular target?
- Threat Type, which addresses the type of malware involved. Is it highly sophisticated or just garden-variety phishing?

In each case, the more sophisticated and targeted the overall threat, the higher the score. The index is based on a massive database of globally observed threats and malware analysis across corporate and consumer email, social media and other platforms.

Once the cyber team has identified their VAPs, they know where to focus their energies. From a technology perspective, that might mean adding security controls around those individuals. From a people perspective, the first step is to train VAPs to recognize phishing attempts and other socially engineered attacks.

The next step is to turn those VAPs into assets for the cyber team. Once an individual is recognizing threats, they can feed that information back to the team, said Brody. "Whereas before, they were one of the weakest links in the chain, we're going to make them one of the stronger links," he said.

Securely Connect and Scale Remote Workforces

With Prisma™ Access

paloalto NETWORKS | PRISMA BY PALO ALTO NETWORKS

paloaltonetworks.com/prisma/access

INDUSTRY SPOTLIGHT

Why the Future of Security Is Cloud Native

An interview with Dan Beaman, Regional Sales Manager for Federal Systems Integrators; and David Knisely, Director of Federal Business Development Capture, Palo Alto Networks

Recent changes in federal cybersecurity policies and standards are positioning agencies to take full advantage of new and emerging capabilities in cloud, mobility and related technologies.

In particular, the recent release of Trusted Internet Connections (TIC) 3.0 and the evolution of the Continuous Diagnostics and Mitigation (CDM) Program provide agencies with a framework for supporting a distributed enterprise that encompasses remote offices and teleworkers. For agencies, the challenge now is to adopt security solutions that provide the scalability and flexibility this environment requires.

To explore the ramifications of this shift, GovLoop spoke with two subject matter experts at enterprise cybersecurity vendor Palo Alto Networks: Dan Beaman, Regional Sales Manager for Federal Systems Integrators, and David Knisely, Director of Federal Business Development Capture.

New Model, New Possibilities

When the Office of Management and Budget launched the TIC initiative in 2010, its goal was to reduce the federal government's attack surface by limiting the number of public internet connections and directing all network traffic through security stacks in the data center.

The limits of the original TIC model became apparent with the emergence of cloud, mobility, the internet of things (IoT) and, more recently, broadband wireless solutions. As applications and data moved to virtualized environments, it no longer made sense to require all traffic to pass through the data center as the original TIC model required.

"Government is recognizing that there are much more robust technologies and security controls that they haven't been able to capitalize on," says Beaman.

One of the use cases of TIC 3.0 is the mobile worker. Thanks to the increased capabilities of mobile devices and increased bandwidth, agencies now have countless users in the field. With TIC 3.0, agencies can provide those users with better performance and security by moving security controls closer to them.

"The CDM Program has also evolved, adding cloud-related security capabilities and data protection management that extends beyond the network perimeters," says Knisely. He adds, "With agencies now shifting 50% or more of their workloads to the cloud, such changes had to happen."

Why Cloud Native Security?

The importance of supporting the remote workforce has become even more apparent during the COVID-19 pandemic, which has led many agencies to allow employees to work from home. The situation also provides a key use case for natively cloud-based solutions.

Most agencies have the capacity to enable some employees to securely telework some of the time, but what happens when a large number of employees need to work remotely all at once and with little notice?

In theory, a cloud-based security solution should provide the necessary flexibility and scalability. However, many so-called cloud solutions were not designed for the cloud but instead retrofitted for it, relying on script languages to provide automated capabilities. Facing a surge in demand, such solutions are "falling down because they don't have the speed and scale to dynamically flex," says Beaman.

Palo Alto Networks Prisma™ Access is a cloud-native secure access service edge (SASE) platform that helps Federal agencies deliver networking and security to branch offices and remote users. Additionally, the company provides Prisma Cloud, a DevSecOps platform that supports the development of cloud native applications.

Both Prisma Access and Prisma Cloud have achieved In-Process designation for the Federal Risk and Authorization Management Program (FedRAMP), working toward a FedRAMP Moderate Agency Authorization.

"Even once the COVID-19 crisis has eased, these kinds of capabilities will be critical to agencies because remote work has become the new norm," Knisely says.

Conclusion

Imagine someone arguing that federal agencies would be better off if they reverted to a perimeter-based network architecture. Not just perimeter-based security, mind you, but an IT architecture in which all users, systems and data reside within the bounds of the data center. No cloud, no mobile devices, no remote offices, unless those offices had their own perimeter-based network architecture.

No one would take such an argument seriously. Whatever the challenges of providing security in the modern IT enterprise, agencies recognize that they have no interest in going back to a 1990s network architecture. As their networks evolve, cybersecurity needs to evolve as well.

And that is what we are seeing. At a recent GovLoop roundtable event, Sean Connelly, the TIC Program Manager, noted that with TIC 2.0, it took 11 months to go from draft to final form. Beginning with TIC 3.0, they are taking a new approach to incorporating evolutionary changes. Rather than putting everything into policy, which requires a lengthy process, they are developing use cases that extend the TIC policy to address new requirements.

The CDM program also is looking to provide agencies with the flexibility they need to address new requirements. CDM's Dynamic and Evolving Federal Enterprise Network Defense (DEFEND) program enables agencies to conduct proofs of concept (POCs) for new security strategies, with the lessons from those POCs being shared with other agencies.

Meanwhile, as noted earlier in this report, GSA is taking a multi-pronged approach to strengthening the FedRAMP program, with a focus on getting new solutions through the authorization process and into use across government more quickly.

Across all three programs, the philosophy is the same: Cybersecurity policy should support, not hinder, agencies as they adopt innovative solutions. Agencies depend on innovation to help them keep pace with evolving mission requirements, so they are looking to cybersecurity to keep pace with innovation.

In short, they are looking for mission-driven cybersecurity.

About Carahsoft

Carahsoft Technology Corp. is The Trusted Government IT Solutions Provider®. As a top-performing GSA Schedule and SEWP contract holder, Carahsoft serves as the Master Government Aggregator™ for many of its best-of-breed technology vendors, supporting an extensive ecosystem of manufacturers, value-added resellers, system integrators and consulting partners committed to helping government agencies select and implement the best solution at the best possible value.

Visit www.carahsoft.com, follow @Carahsoft, or email sales@carahsoft.com for more information.

About GovLoop

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 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 the public sector.

For more information about this report, please reach out to info@govloop.com.

govloop.com | @govloop

Thank You

Thank you to Carahsoft for their support of this valuable resource for public sector employees.

Authors

John Monroe, Director of Content
Mark Hensch, Staff Writer

Designer

Kaitlyn Baker, Creative Manager

CDM Approved Solutions from Carahsoft and our Reseller Partners

The Continuous Diagnostics and Mitigation (CDM) Tools SIN provides products and services from high-quality cybersecurity vendors that enable network administrators to be constantly aware of the state of their respective networks, understand risks and threats, and identify and mitigate flaws at near-network speed.

Each of the following solutions providers have been certified by the CDM program on the approved products list and are available through Carahsoft's reseller partners and GSA Schedule 70, SIN 132-44 (CDM Tools).

Adobe | Akamai | Anomali | BlackBerry Cylance | Bromium | CA Technologies

CyberArk | CyberSponse | Dell EMC | Digital Guardian | Druva | exabeam

F5 | FireEye | ForeScout | ForgeRock | Gigamon | Hitachi

HYTRUST | Imperva | Infoblox | ivanti | Lookout | McAfee

Micro Focus Government Solutions | New Relic | Nlyte Software | okta | paloalto Networks | proofpoint

qmulos | QuantumSecure | Red Hat | RSA | NS2 | Saviynt

servicenow | splunk> | Symantec | Thales | Trend Micro | tripwire

Trustwave Government Solutions | Venafi | Veracode | Veritas | vmware | zscaler

For more information, contact the CDM team at Carahsoft at 855-4-DHS-CDM; CDM@carahsoft.com or visit carahsoft.com/cdm.

carahsoft

Carahsoft's FedRAMP solutions are available through its reseller partners on a variety of contracts including Carahsoft's GSA Schedule 70, SEWP V, ACCENT, NASPO ValuePoint, and numerous state and local contracts. Learn more at Carahsoft.com/FedRAMP.

See the latest innovations in government IT from Carahsoft's vendor partners at Carahsoft.com/Innovation.

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

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop