

Nextgov

Cloud Security

March 2021



Work Securely, Anywhere

Organizations and their teams need the ability to work regardless of location. The success of remote collaboration is dependent on the tools your employees have access to.

Together with our strategic partners, Cisco, HP, Microsoft, and Intel, we can securely support any and every kind of remote work solution.

Empowering the Modern Workforce



Gain Security Insights. Take Actions Faster. IBM Cloud Pak for Security.

IBM Cloud Pak® for Security provides a platform to quickly integrate your existing security tools and generate deeper insights into threats across hybrid and multicloud environments. It allows your organization to connect workflows, orchestrating and automating your security response with a unified interface to meet your mission faster and more securely.

Learn more about how IBM Cloud Pak for Security can help your organization reduce risk and secure your data at www.dlt.com/IBM

DLT®

A TECH DATA COMPANY

Distributor

IBM

Unlock the best of cloud

In a world full of generalists, NetApp is a specialist. We are relentlessly focused on helping you get more out of cloud than you ever thought possible. Whether on premises, in the cloud or anywhere in between, no one integrates, secures and connects your storage like NetApp does.

www.netapp.com

The Cloud Storage Specialist



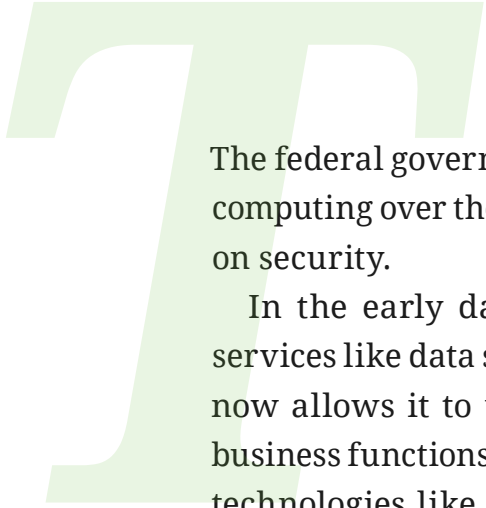


VERITAS[™]

Optimize Your
IT Environment
with APTARE.

Reduce costs.
Reduce resources.
Reduce management.


INTRODUCTION



The federal government's increased and evolving use of cloud computing over the past decade necessitates an equal emphasis on security.

In the early days of cloud, federal agencies used basic services like data storage, but the technology's rapid evolution now allows it to underpin many agency missions. Critical business functions, like email and calendar functions, and data technologies like analytics, machine learning and artificial intelligence, operate optimally in the cloud environments now native to most agencies, elevating the importance of cloud security.

But basic cyber hygiene in remote environments is far from rudimentary or guaranteed. The civilian government's foremost cyber experts at the Cybersecurity and Infrastructure Security Agency have warned of numerous vulnerabilities agencies must address in using cloud computing. And there is confusion among federal technologists about whether agencies or cloud service providers should take responsibility for securing the clouds government data and applications run on.

In this ebook, *Nextgov* examines what is and isn't working in federal cloud security and what the future of the landscape is heading toward. 

Frank Konkel
Executive Editor

TABLE OF CONTENTS

Chapter 1

CISA Warns of Vulnerabilities in Cloud Use

p.4

Chapter 2

House Passes Bill to Codify and Revamp FedRAMP

p.7

Chapter 3

CISA Releases Trusted Internet Connection Use Case for Remote Workers

p.9

Chapter 4

What to Expect from CISA's Continuous Diagnostics and Mitigation Efforts

p.12

Chapter 5

Survey Finds Most Federal Officials Expect Cloud Service Providers to Secure Their Data

p.15

CHAPTER 1

CISA WARNS OF VULNERABILITIES IN CLOUD USE

BASIC CYBER HYGIENE ISN'T SO BASIC WHEN IT COMES TO
REMOTE ENVIRONMENTS.

The Cybersecurity and Infrastructure Security Agency shared 21 bullet points—more for organizations using Microsoft’s Office 365—for diminishing the extent to which adversaries are taking advantage of challenging-to-secure cloud configurations.

[Analysis CISA issued](#) in January draws from incidents the agency has responded to where indicators of compromise show threat actors effectively targeting organizations’ use of the cloud with techniques such as phishing.

While CISA has been responding to federal agencies and private-sector organizations dealing with the fallout from the hacking campaign associated with the compromise of software from IT management firm SolarWinds, the agency noted that the analysis is not explicitly related to that specific threat actor.

CISA “is aware of several recent successful cyberattacks against various organizations’ cloud services,” the analysis reads. “Threat actors are using phishing and other vectors to exploit poor cyber hygiene practices within a victims’ cloud services configuration.”

The term “cyber hygiene” is meant to capture the lowest-common-denominator things

organizations can do to protect their systems from unauthorized access. But remote working conditions necessitated by the pandemic are raising that bar for organizations and highlighting the complexity involved in securely navigating cloud environments.

“These types of attacks frequently occurred when victim organizations’ employees worked remotely and used a mixture of corporate laptops and personal devices to access their respective cloud services,” CISA said. “Despite the use of security tools, affected organizations typically had weak cyber hygiene practices that allowed threat actors to conduct successful attacks.”

Among the list of solutions are measures to protect against phishing. Organizations should “focus on awareness and training,” and ensure employees know how threats can be delivered through such scams, for example. CISA also advised organizations to “establish blame-free employee reporting and ensure that employees know who to contact when they see suspicious activity or when they believe they have been a victim of a cyberattack,” in the interest of more quickly implementing mitigation strategies.



Mariam Baksh
Staff Correspondent

But after initial access is established by obtaining a phishing victim's legitimate credentials, attackers can run rampant undetected, using their access to read emails as well as to identify additional legitimate credentials and reroute messages to their own offsite accounts. Victims had been using the ability—[allowed by Outlook Web App](#)—to have their work emails forwarded to their personal accounts. The attackers also manipulated these forwarding rules to send potential phishing warnings to folders storing RSS feeds, reducing the likelihood they would be seen.

The solution set against these techniques include routinely reviewing user-created email forwarding rules



and alerts, auditing email rules with enforceable alerts, or restricting forwarding and enforcing multifactor authentication.

But attackers are also bypassing multifactor authentication by stepping in imprints left by legitimately credentialed activity. "In this case, CISA believes the threat actors may have used browser cookies to defeat MFA with a 'pass-the-cookie' attack," the agency said.

Among CISA's solutions is to "have a mitigation plan or procedures in place; understand when, how, and why to reset passwords and to revoke session tokens." The MITRE encyclopedia of tactics, techniques and procedures known as ATT&CK lists "configure browsers or tasks to regularly delete persistent cookies" as a mitigation measure.

Users of Microsoft's Office 365 should consider specific mitigations, CISA said. The suite of cloud-based services was specifically named in the Justice Department's disclosure of its compromise by the SolarWinds attackers, and CISA and the National Security Agency have tailored their guidances to

address Microsoft's cloud environment.

"Assign a few (one to three) trusted users as electronic discovery (or eDiscovery) managers to conduct forensic content searches across the entire M365 environment (Mailboxes, Teams, SharePoint, and OneDrive) for evidence of malicious activity," CISA said, among other O365-specific recommendations.

Providers of cloud-based security services weighed in on the increasingly difficult challenge of securing such environments.

"IT staff can be a scarcity—let alone a cybersecurity team," Jim Richberg, Fortinet Public Sector Field CISO, told *Nextgov*.

"Systems are getting more and more complex, which limits the number of folks to verify the fidelity of those systems," added Michael Cardaci, CEO of FedHIVE.

Ben Johnson, former NSA hacker and co-founder and chief technology officer of the firm Obsidian Security, noted: "With the popularity of cloud and how easy it is to become interconnected and scaled, these attacks are not going away." **N**

CHAPTER 2

HOUSE PASSES BILL TO CODIFY AND REVAMP FEDRAMP

THE BILL WOULD PROVIDE \$20 MILLION IN ANNUAL
APPROPRIATIONS FOR THE FEDERAL CLOUD
SECURITY PROGRAM.

The House of Representatives passed legislation in January that would codify and reform the Federal Risk and Authorization Management Program, or FedRAMP.

The program office, created in 2011 within the General Services Administration, provides federal agencies a standardized approach to security assessments, authorizations and monitoring of cloud computing services.

The [FedRAMP Authorization Act](#), sponsored by Reps. Gerry Connolly, D-Va., James Comer, R-Ky., and Jody Hice, R-Ga., aims to address several concerns raised by industry and federal stakeholders over the years, including speeding up the time it takes for cloud solutions to be utilized by agencies.

“The current state of cloud adoption in the federal government involves various agency-specific processes, making it complicated for agencies to issue an authorization to operate for cloud services, even when a cloud service provider has already been authorized for use at other agencies,” Connolly said in a statement. “For nearly four years, I have worked with the Office of Management and Budget, GSA, industry stakeholders, and my friends on the

other side of the aisle to ensure that the bill makes needed improvements to the FedRAMP program, and also gives the program flexibility to grow and adapt to myriad future changes in cloud technologies.”

The bill—one of the first passed by the new 117th Congress—is a virtual copy of legislation passed [twice](#) in the House during the previous Congress. The bill was included as an [amendment](#) to the House National Defense Authorization Act of 2021 but did not make the final version of the bill.

The bill would push GSA to automate processes to promote reciprocity for security validations from one agency to another and would call on the agency to establish a committee to ensure dialog among GSA, agency cyber and procurement officials and industry. In addition, the bill would authorize \$20 million in annual appropriations for the FedRAMP program office. **N**



Frank Konkell
Executive Editor



CHAPTER 3

CISA RELEASES TRUSTED INTERNET CONNECTION USE CASE FOR REMOTE WORKERS

THE AGENCY SOUGHT FEEDBACK ON THE BEST METHODS FOR
SECURING MOBILE AND PERSONAL DEVICES CONNECTING TO
AGENCY NETWORKS.

With many federal employees still teleworking, federal officials dropped a holiday gift for cybersecurity managers across the government: the draft remote user use case for the latest iteration of the [Trusted Internet Connection, or TIC, policy](#).

The Cybersecurity and Infrastructure Security Agency, or CISA, released [the draft use case](#) in December for public comment, asking stakeholders to offer feedback on the best methods for securing mobile and personal devices connecting to agency networks. The late-in-the-year policy drop meets the agency's promise to deliver hard guidance—even if in draft form—before interim guidance released in April expires at the end of December.

The nature of computing has changed a lot since the first TIC policy was issued in 2007, and even since the last update—TIC 2—in 2012. Since that time, the use of cloud and remote computing have skyrocketed, as have security techniques for traditional connections, like at an agency's headquarters office.

To meet these new realities, the Office of Management and Budget issued a [new TIC 3 policy in September 2019](#). But rather than

creating another stagnant guidance document, the policy pushes agencies toward a set of evolving use cases developed by CISA.

“We have the guidebook and the reference architecture documents—we consider those more of the strategic documents, the ones agencies use to build out their understanding of TIC 3 in general,” TIC Program Manager Sean Connelly [told Nextgov in March](#). “And then what we call the operational, the more technical documents: the use cases, the security capabilities and the overlays. We think those are the ones that will be used more by agencies as they build out and secure their environments.”

The main body of the new TIC 3 policy was [finalized in July](#), including the TIC 3 Guidebook; the reference architecture explaining how the concepts should be applied to agency enterprises; and the Security Capabilities Catalog, formerly the Security Capability Handbook.

But the real meat of the policy is in several use cases outlining specific scenarios and how agencies should secure those connections.

The program office released [draft use cases](#)



Aaron Boyd
Senior Editor

in 2019 for traditional connections and branch offices—two of the primary use cases called out in the OMB policy. Remote users and cloud services were also cited in the memo, though CISA officials saw an urgent need to move on the remote use case as federal employees continue to telework en masse in response to the COVID-19 pandemic.

The agency released some [interim telework security guidance in April](#) with the caveat that it was not related to the official TIC 3 policy and a full use case would be published before the end of 2020. A forward in the latest document notes the draft use case will replace the interim guidance.

While the interim guidance offers a number of useful tips for creating secure remote connections to the cloud, the new draft use case expands that to include connections on-premise at agency facilities and to the internet at large.

The new use case outlines how remote users connect to agency networks and resources and highlights the different security enclaves—or trust zones—including the user; the agency; a cloud service provider, if applicable; and the internet at large. The document then outlines how an agency would secure these zones in a traditional context, with relevant alterations to meet the needs of a remote and teleworking workforce.

CISA officials noted the use case broadens the definition of remote users to include employees working on mobile as well as personal devices, also known as bring your own device, or BYOD. This also extends to the use of mobile devices—personal or government-furnished—while physically present in an agency building, per the document.

“The draft use case is designed to help agencies preserve security as they move away from traditional network scenarios in support of the maximized telework environment,” Matt Hartman, acting assistant director of CISA’s Cybersecurity Division, said in a statement. “CISA expects the security guidance will help agencies improve application performance, reduce costs through reduction of private links and improve user experience by facilitating remote user connections to agency-sanctioned cloud services and internal agency services.”

The draft document was open for public comment until Jan. 29. [N](#)



ANDREY SUSLOV / SHUTTERSTOCK

CHAPTER 4

WHAT TO EXPECT FROM CISA'S CONTINUOUS DIAGNOSTICS AND MITIGATION EFFORTS

PROGRAM MANAGERS SAID THE SUMMER WILL BRING
DATA QUALITY CHECKS.

Officials at the Cybersecurity and Infrastructure Security Agency plan to offer a revamped Continuous Diagnostics and Mitigation program that will improve security while relieving agencies' compliance reporting burdens, as intended.

"As we see it, in [fiscal year] '21, we'll really be able to show the promise of CDM," said Kevin Cox, a program manager overseeing updates to the CISA operation.

Cox and fellow CDM program manager Judy Baltensperger spoke during a December event hosted by *MeriTalk* where they detailed their approach, including through pilots with several agencies, to deploying a new dashboard system and accompanying tools by Sept. 30.

CDM initially launched in 2013 with a blanket purchase agreement contract for companies—system integrators—to supply agencies with tools including diagnostic sensors and dashboards so they could more effectively prioritize addressing their vulnerabilities. The system would also feed data automatically being collected from the agencies to a central dashboard to inform a governmentwide assessment of risk by the

Department of Homeland Security.

A big incentive officials articulated for agencies to participate fully in the program is that they would be able to use the data collected by the sensors to inform reports they're required to make to the Office of Management and Budget about their risk management activities.

But a [Government Accountability Office report](#) in August showed that agencies hadn't properly inventoried their equipment. And when the sensors detected and recorded vulnerabilities, the already poor, noisy data did not reflect when they had been mitigated.

Baltensperger said a change in vendors for the dashboard system—they are now using a company called Elastic—as well as new tools and principles, will make the system more efficient and if agencies participate fully, they could lessen the burden from binding operational and emergency directives from CISA.

"We want the data to be as complete and accurate, and as timely as possible, so that we can reduce the data calls for [binding operational directives] and [emergency



Mariam Baksh
Staff Correspondent

directives], reduce the CyberScope reporting, and get them to trust the data in the dashboard when they're making those risk-based decisions," she said.

Baltensperger noted that representatives from pilot agencies, including the Nuclear Regulatory Commission, expressed positive results at a recent customer advisory forum.

"[The official] found that data ingest has been reduced significantly," she said, adding that the integrator "was able to reduce the number of duplicate records for device counts. So the tune-up of the integration layer improves the

completeness and accuracy of the data at his agency and he was so excited we wanted to share with other agencies."

Baltensperger said most of the pilot agencies have plans to move or already have their infrastructure in the cloud and that while related system integrators are currently self-assessing the quality of the data collected in those environments, data quality certification will be done, likely by summer.

"What we want to do through the pilots that we've had engaging with the different CSPs, the cloud service providers," Kox said, "is make sure that

we have a full understanding of the data they have available, look at, for example, how the data that they have available aligns with the CDM requirements. And then make sure that that is available to the agencies, that they have that real-time and near real-time understanding of the protections they have in the cloud."

In terms of new tools, Cox said that with greater use of encryption, endpoint detection and response technology should play an important role.

"With more and more network traffic being encrypted, it's harder to track broadly, all of the different adversarial actions going on," he said. "But at the end of the day, the adversaries are going after the data locations and where users are, so we are looking at endpoint detection and response, EDR, as a key mechanism to help get broader visibility for the agencies."

Cox said a more flexible contracting arrangement is also making all the updates go smoother, and that CISA will continue to work with Congress on the funding piece. **N**



VECTORFUSIONART / SHUTTERSTOCK

CHAPTER 5

SURVEY FINDS MOST FEDERAL OFFICIALS EXPECT CLOUD SERVICE PROVIDERS TO SECURE THEIR DATA

REPORT VALIDATES FEDERAL OFFICIALS' CONCERNS ABOUT
INACCURATE ASSUMPTIONS IN THE NEW ENVIRONMENT OF
"SHARED RESPONSIBILITY."

U.S. federal agencies are leading global counterparts and private sector entities in digital transformation, but their use of cloud services and connected devices brings risks they're not appropriately adjusting to, according to an annual survey of threats to data security.

"When it comes to securing data in the cloud, most government organizations incorrectly look to their cloud providers to implement data security measures for the portion of the shared responsibility model that is owned by the government organizations themselves," reads the federal edition of the 2020 Thales Data Threat report.

[The report](#), released in April, is sponsored by the Cloud Security Alliance and companies offering just the type of data security and information technology services it recommends federal agencies increase investments in. But it highlights a dynamic which [key government officials also recently flagged](#): Federal administrators may be relying on cloud providers to perform actions for which the administrators themselves are accountable.

The federal edition of the report is based on

a survey of 101 U.S. government respondents which the International Data Corporation, an analytics firm, conducted in November 2019. It compares the U.S. government perspective to those of public and private sector entities in 16 countries collected through a larger survey of 1,723 individuals.

While the U.S. government respondents were the most confident about their security, U.S. federal agencies have been breached at higher rates than the global sample, according to the report.

Almost 30% of federal respondents reported breach incidents within the last year, according to the survey.

"The more digitally transformed an organization, the more likely that it has experienced a data breach," the report reads. "Digitally Determined organizations (those organizations making the strategic, organizational, technological, and financial decisions that will set them up to digitally transform their organization in the next several years) may also have greater data threat exposure."

There is one big caveat. Entities with a



Mariam Baksh
Staff Correspondent



greater level of sophistication may also be more aware they have been breached, the report notes, while less sophisticated organizations may be less exposed or may have been breached without knowing it.

Regardless, the report recommends a greater focus on data security—which it differentiates from network or application security—and highlights shortcomings in encryption practices. Almost all of U.S. government respondents said at least some of their sensitive data in the cloud is not encrypted, according to the report.

“More than half of U.S federal government data [54%] is now stored

in the cloud, with a significant portion of that data being sensitive,” the report reads. “As a result, IT security departments must now, more than ever, embrace and own their portion of the cloud shared responsibility model and implement data security best practices, as the cloud provider most often does not guarantee security at the data level.”

The report adds, “U.S. federal government respondents are seemingly less worried about issues over which they have direct control, and which represent greater potential vulnerabilities, like encryption key management.”

The National Institute of Standards and Technology’s Matthew Scholl also flagged a need to focus on the management of cryptographic keys during an event noting federal agencies’ rapid migration to the cloud in response to increased remote work needs during the coronavirus pandemic.

Scholl and the report both also stressed the importance of user access controls given the proliferation of new endpoints being added to networks, with the report noting that insider threat is “often more about carelessness than malicious behavior.” **N**

MEET THE CONTRIBUTORS



MARIAM BAKSH

STAFF CORRESPONDENT

Mariam Baksh reports on the development of federal cybersecurity policy for *Nextgov*. She started covering technology governance in 2014, during the heat of the Net Neutrality debate, and focused her graduate studies at American University on investigative journalism.



FRANK KONKEL

EXECUTIVE EDITOR

Frank Konkel is *Nextgov's* executive editor. He writes about the intersection of government and technology. Frank began covering tech in 2013 upon moving to the Washington, D.C. area after getting his start in journalism working at local and state issues at daily newspapers in his home state of Michigan.



AARON BOYD

SENIOR EDITOR

Aaron Boyd is an award-winning journalist currently serving as senior editor for technology and events at *Nextgov*. He primarily covers federal government IT contracting and cybersecurity issues affecting both civilian and defense agencies.

Nextgov