GovCIO
MEDIA & RESEARCH

DeepDives

What Happens After a Breach?

INSIDE:

Congress Mandates Cyber Incident Reporting 3

Why Internal Risks are the Biggest Threats 8

Data Silos are a Risk 12

SPONSORED BY exterro®

GovCIO
MEDIA & RESEARCH

From the writer's desk

Kate Macri, Senior Staff Writer

So you've been hacked. Now what?

That's the question federal and industry cyber leaders have been trying to answer in a simple, standardized way over the past year. It's not as easy as calling the 911 of cyber — Cybersecurity and Infrastructure Security Agency (CISA) — and it's not always clear who else you should notify in the event of a data breach, whether that be vendors, suppliers or other federal agencies, such as the FBI.

In its 2022 budget signed by President Joe Biden in March, Congress mandated cyber incident reporting to CISA within 72 hours. That requirement brings sharp relief to the question of what to do after a cyberattack.

As organizations shore up defenses with zero trust strategies and associated identity management solutions, federal agencies and industry are working together to develop a consistent framework for responding to cyberattacks so you can limit the damage and protect business partners.

Table of Contents

Kate Macri,
Senior Staff
Writer

ARTICLE

CISA, Cyber Incident Reporting Mandates Get Billions in Congressional Budget

The spending boost and new requirement come as U.S. critical infrastructure sectors prepare for more cyberattacks.

BY KATE MACRI

INFOGRAPHIC

What to Do After Discovering a Breach

PARTNER INTERVIEW

Reacting to a Cyberattack

As cyberattacks and ransomware attacks multiply, federal agencies need to have response strategies in place to mitigate damage and alert others who may be impacted.

Exterro Forensic Subject Matter Expert Justin Tolman

BY KATE MACRI

ARTICLE

A Common Cyberattack Mistake is Not Reporting Quickly Enough

CISA encourages all organizations to report immediately and maintain consistent communication until cyber incidents are resolved.

BY KATE MACRI

ARTICLE

Centralizing Cyber Ops Necessary as Cyberattacks Escalate

DHS cyber leaders have a laundry list of items for federal CISOs to address.

BY KATE MACRI

ARTICLE

Cyber Incident Reporting Key to Robust Federal Security Strategies

Cyber incident reporting takes center stage as federal cyber leaders tackle recent security incidents.

BY KATE MACRI

GovCIO MEDIA & RESEARCH

CISA, Cyber Incident Reporting Mandates Get Billions in Congressional Budget

The spending boost and new requirement come as U.S. critical infrastructure sectors prepare for more cyberattacks.

BY KATE MACRI

Critical infrastructure companies including water, wastewater and energy utilities, nuclear reactors and nuclear waste facilities, hospitals and other health care organizations, IT companies such as cloud service providers, the Defense Industrial Base (DIB) and others will be required to report cyber incidents within 72 hours to the Cybersecurity and Infrastructure Security Agency (CISA), according to the fiscal year 2022 government funding bill Congress dropped early March.

DOD CISO David McKeown

The $1.5 trillion spending package allocates $2.59 billion for CISA to address cyberthreats facing U.S. critical infrastructure sectors, granting the agency $300 million more than the Biden administration's budget proposal.

The new cyber incident reporting requirement comes as the U.S. braces for potential malicious cyber activity due to Russia's invasion of Ukraine and after nearly a year of calls from federal cyber leaders to mandate cyber incident reporting and information-sharing in order to better address and prepare for cyberattacks against the nation's critical infrastructure sectors.

The requirement also comes just weeks after the Defense Department Inspector General found that some academic and research contractors within the DIB "did not consistently implement cybersecurity controls in accordance with federal and DOD requirements for safeguarding controlled unclassified information (CUI)."

The contractors reviewed by the DOD IG did not enforce multi-factor authentication, mitigate vulnerabilities "in a timely manner," monitor network traffic or scan for viruses, or disable users after designated periods of inactivity on the network, according to the Feb. 22 report, due to DOD contracting officials' failure to verify contractors' compliance with the National Institute of Standards and Technology (NIST) special publication 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations."

DOD CISO David McKeown said during a DOD town hall Feb. 24 he wants the DIB to report cyber incidents to the DOD Cyber Crime Center (DC3) within 72 hours. He encouraged defense contractors to "go beyond" reporting

Photo Credit: Lisa Ferdinando, Office of the Secretary of Defense Public Affairs/DVIDS

Brandon Wales

Executive Director, CISA

requirements due to the pervasiveness of malicious cyber activity and to review NIST special publication 800-171.

“I think we’ve thwarted a good number of attacks by our intelligence sharing and your sharing of information about things going on in your network,” he said during the town hall.

McKeown’s comments joined the chorus of critical infrastructure sectors and other federal cyber leaders calling for cyber incident reporting requirements over the past year.

FireEye (the cybersecurity firm that discovered the SolarWinds software supply chain breach), the Information Technology Industry Council (ITI), USTelecom and the American Gas Association urged Congress to mandate a flexible 72-hour window for cyber incident reporting during a House Homeland Security Committee hearing in September 2021.

CISA Director Jen Easterly and Executive Director Brandon Wales also repeatedly asked Congress to mandate cyber incident reporting to CISA last year.

“We need the information to engage with the victim, offer our assistance, understand what’s happening on their networks and protect other victims,” Wales said during a House Oversight Committee hearing in November 2021. “Even today there is a lot we’re doing across the U.S. government to improve our public-private partnership and enable more cyber defensive activities to protecting the homeland. JCDC (the Joint Cyber Defense Collaborative) brought together the critical government agencies and those companies in the private sector that have the best visibility into the cyber ecosystem. These are companies that can take action on a massive scale.”

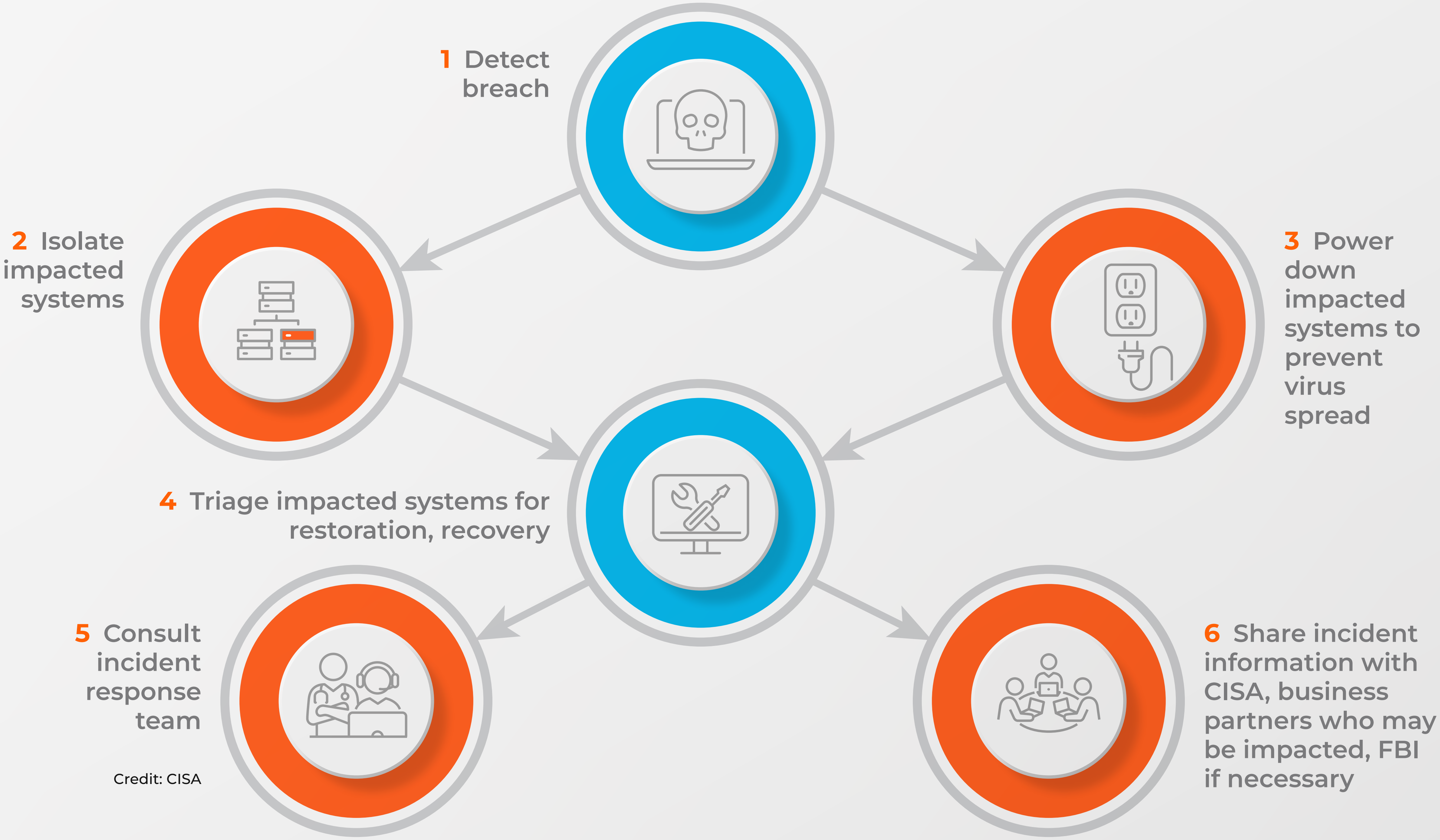
Easterly’s JCDC initiative, launched in August 2021, aims to improve information-sharing around cyber threats and incidents between private and public sector partners, but Wales said requiring critical infrastructure companies to report incidents is another necessary step.

(ctd.)

> “We need the information to engage with the victim, offer our assistance, understand what’s happening on their networks and protect other victims.”
>
> **—Brandon Wales, Executive Director, CISA**

The government funding bill also dedicates $10.7 billion in funding to the Federal Bureau of Investigation (FBI) and requires the director of the FBI to develop a cybercrime database within the FBI’s Uniform Crime Reporting program.

What to do after discovering a breach



1 Detect breach

2 Isolate impacted systems

3 Power down impacted systems to prevent virus spread

4 Triage impacted systems for restoration, recovery

5 Consult incident response team

6 Share incident information with CISA, business partners who may be impacted, FBI if necessary

Credit: CISA

exterro®

GovCIO MEDIA & RESEARCH

PARTNER INTERVIEW

Reacting to a Cyberattack

As cyberattacks and ransomware attacks multiply, federal agencies need to have response strategies in place to mitigate damage and alert others who may be impacted.

Exterro Forensic Subject Matter Expert Justin Tolman

There is a cyberattack every 39 seconds, according to CISA. Gen. Paul Nakasone, director of the National Security Agency and commander of the U.S. Cyber Command, called ransomware a national security threat in 2021. In remote, cloud-based work environments, organizations face more cyber threats than ever before. According to solutions security provider Exterro, learning to develop agile cybersecurity responses and share relevant incident information quickly can help organizations stop attacks in their tracks and protect others.

What is the first thing a federal agency should do when they realize its network has been breached?

Justin The first thing that should happen when a breach is detected is to begin communicating with the relevant departments. Many times a breach is detected and the department may immediately go into their remediation steps. Valuable time and resources may be saved when notification becomes the first step. While notifications are going out, all known resources that have been breached should be isolated immediately to prevent the spread of the breach.

Federal agencies often handle large amounts of data, including public health data, criminal justice data and intelligence data. What are some of the legal and privacy risks federal agencies should consider when they experience data breaches?

Justin The breach of personal data is always a large financial and reputational risk to

(ctd.)

any agency storing such information. However, federal agencies should make sure that their own policies and procedures are complying with the highest mandated standards to avoid any unnecessary risk. One of the largest risks to any type of data is internal. Security models such as Zero Trust can help mitigate even accidental breaches by restricting access to information from both people and services.

How can data visualization and continuous monitoring help federal agencies prevent and recover from cyberattacks?

Justin Little problems require little fixes. Constant monitoring and sharing of information between agencies can help detect and stop breaches when they are small, reducing risk, damage and data loss. Constant monitoring also shows a willingness within the agency to do what is necessary to protect their data.

How critical is cyber incident reporting, and should federal agencies immediately notify vendor partners as well as CISA?

Justin This is very important and even addressed in a presidential executive order on zero trust. Federal agencies should be communicating with each other and vendors not only that the breach occurred, but also the details so that all can benefit and be protected together. Bad actors are constantly sharing information on forums and message boards, why should the "good guys" remain so isolated?

> **"Bad actors are constantly sharing information on forums and message boards, why should the 'good guys' remain so isolated?"**
>
> **—Justin Tolman, Forensic Subject Matter Expert, Exterro**

GovCIO
MEDIA & RESEARCH

A Common Cyberattack Mistake is Not Reporting Quickly Enough

CISA encourages all organizations to report immediately and maintain consistent communication until cyber incidents are resolved.

BY KATE MACRI

One of the most common pitfalls organizations face after a cyberattack is not reporting the incident immediately to CISA, either because they're waiting for "the perfect time" to report or because they're unsure about the severity of an incident.

Cyber incident reporting to CISA within 72 hours of an incident, a practice mandated in Congress' 2022 federal funding package and signed into law by President Joe Biden, is a key post-attack step for organizations after isolating impacted systems and datasets.

"Given the severity of a lot of the cyberattacks we've seen over the last several years, acting quickly to inform and communicate and bring others into it is really important," said CISA Cybersecurity Division Associate Director Michael Duffy in an interview with GovCIO Media & Research. "Some can get stuck in terminology, such as, is this technically an incident and should we dig in a little bit and report tomorrow so we have more to report. Very closely related to that is thinking that just one report is sufficient — the best way we at CISA can gain insights and [provide] tailored support is open that line of communication. CISA is very interested in how things were resolved and what you've seen on the other side as we are at the very beginning of the suspected incident itself."

Another common mistake is resuming normal operations too quickly after an incident. Organizations should take the time to conduct a "full analysis and remediation response" before bringing systems back online, Duffy said. This helps organizations ensure the threat is eradicated, but also prevent similar future breaches.

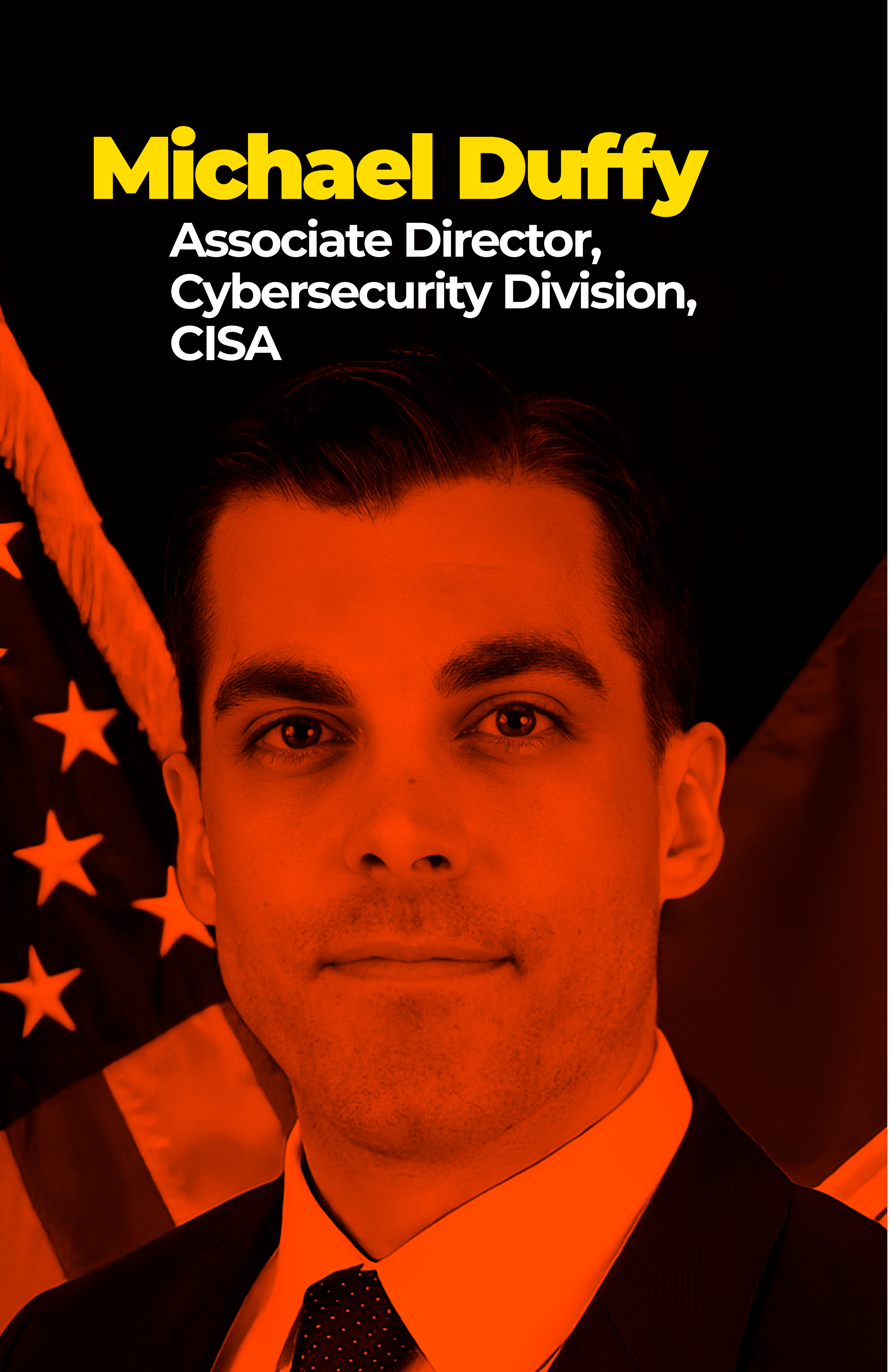
YOUR PERSONAL FILES ARE ENCRYPTED
Make payment or private key will be destroyed in
12 Hours 01:34
YOUR PERSONAL F
ARE ENCRYPTE
Make payment or private ke
will be destroyed in
12 Hours 01:34

Photo Credit: Andrey Popov/iStock

"We in the federal government have been investing a lot in endpoint detection and response solutions to help us gain that greater asset visibility so we can say, we know what the adversaries are after and are able to further

Michael Duffy

Associate Director, Cybersecurity Division, CISA



protect by applying what we've seen across the board," Duffy said.

With the 200% rise in ransomware attacks over the past two years and renewed cyber threats from Russian actors relating to the Russian invasion of Ukraine, businesses and federal agencies face increasingly severe cyber threats, from ransomware to phishing attacks.

Isolating and containing a cyberattack, preserving as much data as possible, and communicating with CISA as frequently as possible are critical steps to limiting the scope of the attack and protecting others.

"Things are so connected for ease of use and access so that what may have been a fairly isolated incident in the past is now fairly widespread if not triaged and isolated appropriately," Duffy said. "Understanding how your system is connected is really important before taking too many steps forward as part of the recovery/response practice."

The rise of remote work due to the COVID-19 pandemic interconnected networks and IT systems more than ever before, highlighting the importance of a zero trust approach to cybersecurity (also mandated by the White House in its May 2021 executive order).

Zero trust is especially critical given the recent prevalence of identity-related attacks, Duffy said, such as the SolarWinds incident in December 2020.

Despite malicious Russian actors exploiting poorly configured multi-factor authentication (MFA) protocols in a recent incident, Duffy said MFA within a zero trust framework "is one of the most important cyber practices that any organization can implement" because it reduces the risk of compromise by 99%.

"This does not call into question zero trust practices or principles at all, in my opinion, it really does say … this is a good example that one pillar of zero trust isn't enough, it's a comprehensive application of zero trust principles [that] is a challenge for organizations," Duffy said. "The path to zero trust is not simple. Finding those little targets, like configuring MFA properly, making sure

> **“We are always worried about the threat of vigilance fatigue. We have been, as a government and a nation, when it comes to cybersecurity, on high alert for almost two years. Our reporting protocol is fairly simple and straightforward via the website: fill out a form and send it in. Keep those lines of communication open.”**
>
> **—Michael Duffy, Associate Director, Cybersecurity Division, CISA**

you have proper identity infrastructure and looking at ways to segment your network so that even one breach, or if one defense mechanism fails, you’ve segmented enough to isolate and prevent a widespread breach across your enterprise. That really matters when we talk about critical infrastructure and high-value assets.”

CISA offers a wealth of resources on its website for organizations seeking cyber guidance and threat information. CISA’s Shields Up webpage, which Duffy said is the most visited webpage on the site right now, publishes the latest updates regarding cyber incidents and emphasizes good cyber hygiene practices, which Duffy said is the most important thing any organization can do to reduce cyber risk.

While reporting incidents immediately to CISA and communicating updates throughout incident response is highly important, Duffy said CISA doesn’t want to “burden” organizations with a multitude of guidance and requirements or make the question of, what to do after a cyberattack, more confusing.

The No. 1 step to remember in the event of a breach? Tell CISA, and keep communicating with CISA until the incident is resolved. CISA can also help organizations determine if or when to notify supply chain partners, contracting partners, or other federal agencies, such as the FBI.

“We are always worried about the threat of vigilance fatigue,” Duffy said. “We have been, as a government and a nation, when it comes to cybersecurity, on high alert for almost two years. Our reporting protocol is fairly simple and straightforward via the website: fill out a form and send it in. Keep those lines of communication open.”

GovCIO MEDIA & RESEARCH

Centralizing Cyber Ops Necessary as Cyberattacks Escalate

DHS cyber leaders have a laundry list of items for federal CISOs to address.

BY KATE MACRI

Cyber leaders say federal agencies should break down information silos, centralize their cyber operations, and use data to drive security decisions in order to barricade their networks against hackers.

Agencies "have made tremendous progress" on strengthening their defenses in the past few years, but cyber criminals and nation-state actors are becoming "more sophisticated and brazen," said Matt Hartman, deputy executive assistant director of cybersecurity at the Cybersecurity and Infrastructure Security Agency.

"We ended 2020 facing one of the most sophisticated supply chain compromises to date," Hartman said at a June 2021 ATARC event in reference to the SolarWinds breach. "We're seeing a ramp-up in frequency and complexity of an already concerning cyber landscape."

SolarWinds headlined one of three emergency directives issued by CISA in the first half of 2021, signaling an unprecedented uptick in cyber activity compared to previous years. Hartman advised federal agencies to step up information-sharing with CISA regarding vulnerabilities and incidents. The sooner CISA knows what's happening, the sooner CISA can warn other entities, provide guidance and help secure networks.

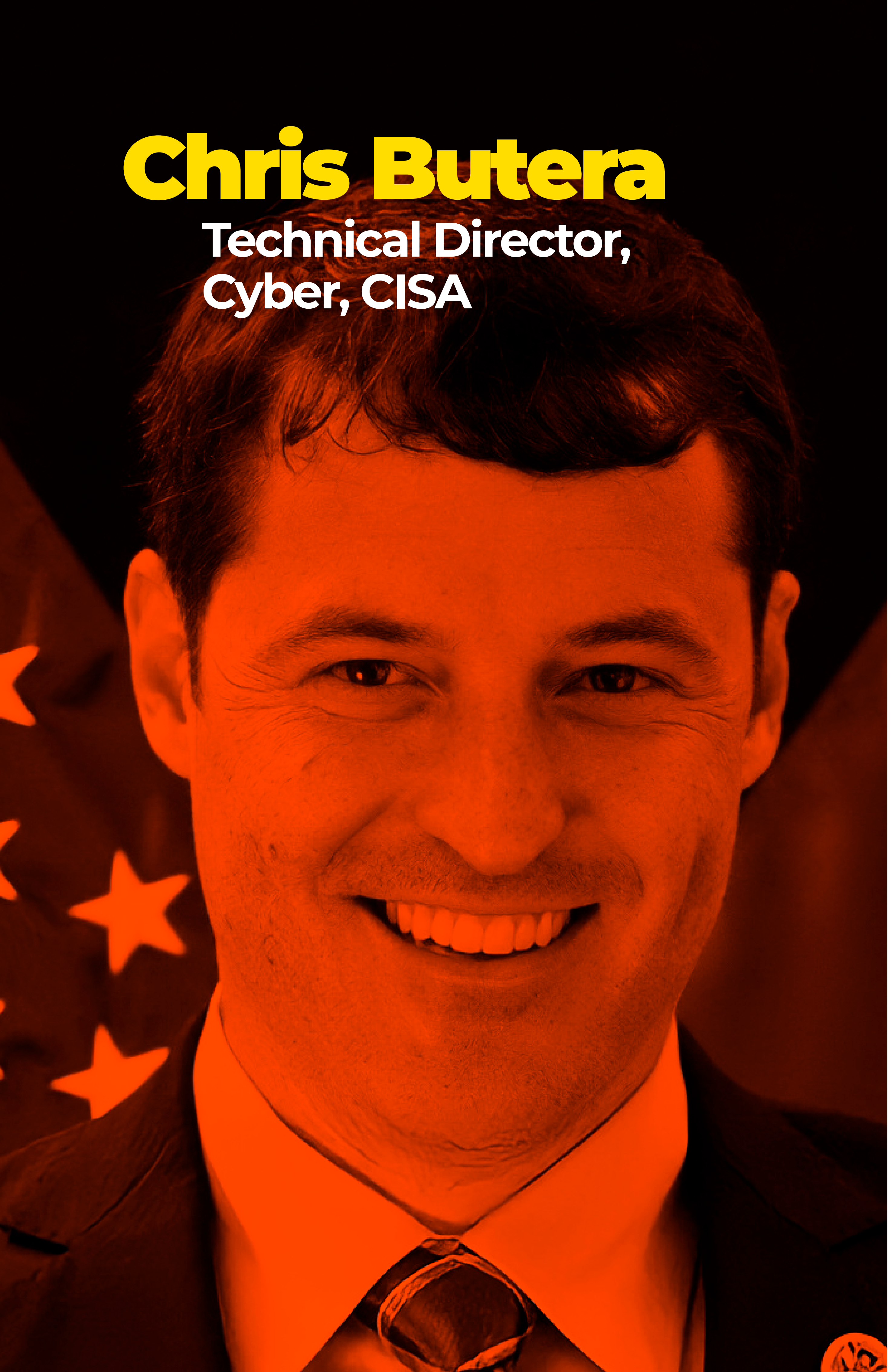
Private and public sector collaboration is another imperative.

"We need to remove barriers to information-sharing in the government and private sector," Hartman said. "Industry is often uniquely positioned to see vulnerabilities or breaches first. IT service providers need to share information with the government and even be required to do so in the event of certain breaches."

Photo Credit: Cecilie_Arcurs/iStock

Federal agencies migrating their IT operations to the cloud face potentially higher cyber risks as they relearn cybersecurity within the context of the cloud.

Shane Barney, CISO at Citizenship and Immigration Services, said the agency's shift from legacy IT infrastructure to the cloud prompted him to



Chris Butera

Technical Director, Cyber, CISA

rethink cybersecurity in terms of security versus risk operations.

Data-driven decision-making is a buzzy phrase for federal agencies modernizing their IT, but Barney challenged federal agencies to apply that same principle to their cybersecurity operations.

“Your security has to match (your scale and scope), so we have a very proactive risk-based organization,” Barney said. “Data-driven security, this is more behavioral-based like threat-hunting, but extending those not just to specialized teams but across your security enterprise. Start with your system operators and give them toolsets and techniques to do threat-hunting at all levels.”

USCIS leads DHS components in its adoption of Agile methodology and DevSecOps, from which Barney learned an important lesson about preventing cyber information silos.

“Something we got from the Agile development world is feedback loops,” he said during the ATARC event. “Ensuring all these processes have some sort of feedback into an organization for security ops. This really drives home the point of automation. Data in the cloud is immense. We take in eight terabytes of data in a single day. Automation becomes critical to your operations.”

Barney began building a cyber threat intelligence platform two and a half years ago, which helped USCIS centralize cyber ops and weather the effects of the SolarWinds breach. Constantly innovating your security program is a must, Barney said.

“The need to innovate within security is so critical,” he said. “We have a bad tendency to say, ‘Oh this is a good tool, we’ll use it for the next 25 years,’ and it becomes obsolete well before then. Checkboxes don’t equal security. That shouldn’t be a hallmark or an indication of how secure something is or is not.”

One of the major cyber challenges facing federal agencies as they migrate to the cloud is open source code risk. Federal agencies now worry less about hardware risks, but need to worry more about software risks and software supply chain security.

> **“If you can contain that cyber incident from spreading to your entire enterprise, recovery can be much quicker, as well as having a plan to operate if your IT enterprise is not possible.”**
>
> **—Chris Butera, Technical Director, Cyber, CISA**

“Code is also a part of the supply chain, we’ve leveraged a lot of open source code in our organization and have had trouble with that,” Barney said. “That becomes a really critical area you have to watch out for. We had a couple of close calls there.”

Chris Butera, technical director for cyber at CISA, said federal agencies should focus on basic cyber hygiene measures and information-sharing before addressing their cloud software supply chains.

“The federal government has renewed momentum in addressing this,” he said during the ATARC event. “What we try to do for all organizations is take a resilience-based approach to cyber incidents. If you can contain that cyber incident from spreading to your entire enterprise, recovery can be much quicker, as well as having a plan to operate if your IT enterprise is not possible.”

HOW DO YOU IMPLEMENT THE FEDERAL MANDATED **ZERO TRUST** FRAMEWORK AND EFFECTIVELY PERFORM REMOTE ENDPOINT DFIR INVESTIGATIONS?

with Exterro **FTK Enterprise**

FTK
ENTERPRISE

Perform a live preview and collect triaged data from remote endpoints, saving countless hours during time-sensitive investigations.

The Exterro endpoint agent works together with your **Zero Trust** agent for seamless operability.

exterro®

LEARN MORE ABOUT THE POST BREACH FEATURES IN **FTK ENTERPRISE** IN OUR LATEST PODCAST

bit.ly/ftk-pod

GovCIO
MEDIA & RESEARCH

Cyber Incident Reporting Key to Robust Federal Security Strategies

Cyber incident reporting takes center stage as federal cyber leaders tackle recent security incidents.

BY KATE MACRI

Congress and the White House are drilling down on increased transparency around cyber incidents and cyber incident reporting at federal agencies and private companies as cyberattacks surge.

In an August 2021 White House memo, OMB Acting Director Shalanda Young outlined a maturity model for federal agencies to track information logs from their IT systems and requirements for information-sharing with the Cybersecurity and Infrastructure Security Agency (CISA) following cyber incidents.

Agencies have two years to reach the highest level of information log maturity, but starting immediately, must begin sharing information logs with CISA following cyber incidents, according to the memo.

“Recent events, including the SolarWinds incident, underscore the importance of increased government visibility before, during and after a cybersecurity incident,” Young wrote in the memo. “Information from logs on federal information systems (for both on-premises systems and connections hosted by third parties, such as cloud services providers) is invaluable in the detection, investigation and remediation of cyber threats.”

A new draft bill from the House Homeland Security Committee amends the Homeland Security Act of 2002 to install a Cyber Incident Review Office within CISA.

Photo Credit: Umnat Seebuaphan/iStock

Most federal agencies and their private-sector partners agree there should be a framework for cyber incident reporting, but some are concerned about legislating a reasonable timeline for reporting incidents to CISA. During a panel hearing with the committee, witnesses from FireEye (the cybersecurity firm that discovered the SolarWinds breach), the Information Technology Industry Council (ITI), USTelecom and the American Gas Association urged Congress to mandate a flexible 72-hour window for reporting.

This time range allows “the operator more time to gather valuable useful

Heather Hogsett
Senior Vice President, Bank Policy Institute

information rather than just spitting information to CISA when CISA is going to come back and ask more questions anyway," said Kimberly Denbow, managing director for security at the American Gas Association. In her prepared testimony, she also argued for prioritizing incident response over compliance.

Heather Hogsett, senior vice president at the Bank Policy Institute, warned against dumping information on CISA for the sake of compliance.

"CISA is deluged with information that's not helpful to them, not useful, and gets bogged down with information that isn't the actual highest threat and risk that we want them and everyone else to focus on," she said at the hearing. "Beyond this scope, setting up a process where there is a regular feedback loop … if we can close that so that CISA has real-time valuable information for them to help them improve their operations, those would be key pieces. The way the bill is drafted allows for that, but your role as you oversee that would be a critical thing we'd highlight."

CISA also released an insights report for federal agencies with outsourced IT this week, highlighting information-sharing and incident reporting as a key item for federal agencies and private-sector partners to discuss.

Clear expectations around information-sharing and cyber incident reporting should be discussed before signing a contract, CISA said in the report.

“CISA is deluged with information that’s not helpful to them, not useful, and gets bogged down with information that isn’t the actual highest threat and risk that we want them and everyone else to focus on. Beyond this scope, setting up a process where there is a regular feedback loop ... if we can close that so that CISA has real-time valuable information for them to help them improve their operations, [that] would be key.”

— Heather Hogsett, Senior Vice President,
Bank Policy Institute