GovCIO
MEDIA & RESEARCH

SPRING 2024

DeepDives

STRENGTHENING CYBER INCIDENT RESPONSE

SPONSORED BY

AXONIUS FEDERAL

INSIDE:

GovCIO
MEDIA & RESEARCH

From the editor's desk

Ross Gianfortune, Managing Editor

Responding to a Cyber Incident is Collaborative

Cyber criminals are increasingly targeting critical infrastructure like the electrical grid, water systems and other entities. Agencies must comply with incident reporting standards as part of White House cybersecurity policy initiatives, with the Department of Homeland Security working to make cyber incident reporting and resiliency easier and more effective for everyone.

At agencies like the Environmental Protection Agency and General Services Administration, having a prepared workforce is integral to building cyber resiliency throughout all levels of an organization.

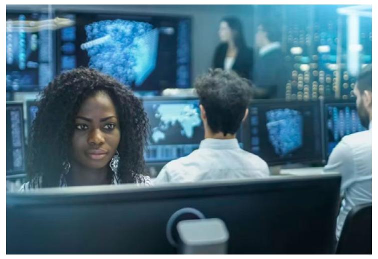
Reporting incidents remains complex and cumbersome, and DHS is trying to ameliorate this problem with a new proposed rule.

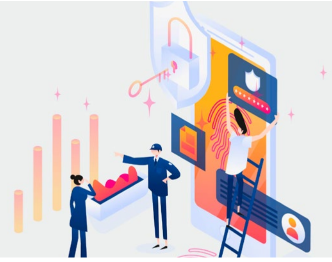
Table of Contents

Amy Kluber,
Editor-in-Chief

Ross Gianfortune,
Managing Editor

Silvia Oakland,
Staff Writer





GovCIO MEDIA & RESEARCH

A Prepared Workforce is Key to Cyber Resiliency

Strong training strategies and emphasizing cyber hygiene basics enhance security practices at federal agencies.

BY SILVIA OAKLAND

Federal agencies are increasingly investing in the cybersecurity workforce to support ongoing zero trust and continuous monitoring goals.

One of the biggest issues is how to ensure the workforce can remain vigilant against persistent threats. Environmental Protection Agency (EPA) Office of Information Security and Privacy Deputy Director Mark Bacharach said building a resilient enterprise starts by training and preparing employees to know what to look for in cyberattacks.

"We have to really help them break down potentially complex ideas to simple things, so they don't have to know all the technology, but they just have to be aware of those risks and then make good decisions," Bacharach said during a GovCIO Media & Research panel.

The EPA has taken on a returning to "cybersecurity basics" approach and removed unauthorized user accounts within the enterprise that could pose security threats, he said. Using a zero trust strategy, the EPA evaluates threats at every level and assesses the maturity levels of the agency.

"We're taking those things that we need to implement, to comply with a zero trust maturity model or to meet it. And then we regularly routinely assess it to determine what's working, what's not," Bacharach said. "Our plan in general is to reinforce success."

Continuous monitoring enables the agency to focus on new threats from bad actors and empowers the workforce to report cybersecurity incidents, based on CISA's guide co-released with FEMA in January.

(ctd.)

Photo credit: Gorodenkoff/Shutterstock

Mark Bacharach

Deputy Director, Office of Information Security and Privacy, EPA

"Almost in the rearview mirror are the days when our employees are falling for free Amazon gift cards or AirPods," Bacharach said. "The practices that are being used today are becoming harder and more complex. We have to train like we're going to fight and use the methods and techniques that are applied against us internally to simulate the environment."

The Energy Department has also partnered with CISA following cyberattacks within the electrical grid in 2022. By mid-2023, CISA said it has alerted 60 entities within energy, health care, water/wastewater and others about potential cyber and physical risks. Sharing information and data about potential or current cyber risks with partners has ensured there is bidirectional sharing and up-to-date threat information.

Emerging technology is showing promise for enabling agencies to be nimble while keeping systems secure. The State Department plans to use emerging technologies like AI and virtual reality for cybersecurity. Bureau of Global Talent Management CTO Don Bauer has been advocating for using AI to monitor threats in order to allow the workforce to focus on mission objectives.

"I have a staff of five on my security team. … We cannot monitor every single log entry," Bauer said at said at a recent conference. "These are opportunities for AI to really start to add benefit, if nothing else, to point out things that just don't look right."

Bacharach said EPA is working to update policies based on President Biden's AI executive order to prepare the workforce to assess and report cyberattacks.

"We're working to put together some updated policy so that we can both comply with [the executive order] and make that those capabilities available," Bacharach said. "But at the same time put together some guardrails, whether it's some updated training materials, so employees understand what are the potential pitfalls and how they can perform appropriate due diligence [or guidance on] using them safely and securely."

> “We’re taking those things that we need to implement, to comply with a zero trust maturity model or to meet it. And then we regularly routinely assess it to determine what’s working, what’s not. Our plan in general is to reinforce success.”
>
> — Mark Bacharach, Deputy Director,
> Office of Information Security and Privacy, EPA

GovCIO
MEDIA & RESEARCH

DeepDives

Recommendations to Harmonize Cyber Incident Reporting

The Department of Homeland Security outlined ways to best report cyber incidents to the federal government. The report suggests eight recommendations related to defining reportable cyber incidents, clarifying the timing and triggers for reporting, leveraging common data elements and developing mechanisms for reporting incidents.

STEP 01

Adopt a model definition of a reportable cyber incident wherever practicable.

STEP 02

Adopt model cyber incident reporting timelines and triggers wherever practicable.

STEP 03

Consider whether a delay in public notification of an incident is warranted.

STEP 04

Adopt a model reporting form for cyber incident reports wherever practicable.

STEP 05

Assess how best to streamline the receipt and sharing of incident reports and cyber incident information.

STEP 06

Incident reporting requirements should allow for updates and supplemental reports.

STEP 07

Adopt common terminology regarding cyber incident reporting wherever practicable.

STEP 08

Improve processes for engaging with reporting entities following the initial report of a cyber incident.

Source: U.S. Department of Homeland Security

PARTNER INTERVIEW

AXONIUS FEDERAL

Accelerating Cyber Incident Response

An accurate cyber asset inventory can simplify reporting requirements.

What is challenging about responding to a cyber incident and what are some ways of simplifying the process?

Schneider You cannot successfully execute the later stages of the incident response pipeline without getting an accurate baseline of the entire environment. Having an accurate and comprehensive asset inventory and data logs available after the incident triage makes response and remediation much quicker and simpler.

While some organizations have invested in the right tools and people to create and maintain the essential inventory and data sets, many others find this challenging due to underfunding.

Sometimes if an agency has not had a serious incident for several years, it's hard to convince management to fund the proper tools to simplify asset inventory. It's easier to get funding for tools for eradication, containment and recovery since they are the most visible stages in incident response. But investments in preparation and protection can reduce the damage from an incident and simplify response and recovery.

The cyber asset inventory really tells you what the battlespace looks like because the different tools and platforms that collect all logs, data metrics and network sensors might not talk to each other. (ctd.)

John Schneider
Senior Systems Engineer,
Axonius Federal

What are some ways to accelerate the time to investigation and remediation in federal environments?

Schneider Many agencies are still using manual processes and spreadsheets, siloing teams and spending hours or even days trying to create an asset inventory. These processes are not fast or scalable, and these manually compiled reports are not always accurate.

Even some of the most popular response tools cannot give a complete picture of the environment because they cannot see what they are not hooked up to.

What can accelerate incident response is having unified data, which requires more than one tool. Having a single point of truth that pulls together the relevant data from all the different tools is key.

One thing we do at Axonius, working together with other vendors, is show what everything in the environment looks like at the current moment. We can also roll back the clock and show you what was already being exploited before the public notice of an incident was sent out.

By rolling back the clock, you can see what you had in place at the time because certain things may have rolled off or on the network after the incident. This process can really help you accelerate the investigation. You then have a

> **"AI will have the same problem as a cybersecurity analyst if they are not given a complete and comprehensive data set. That's why investing in the right tools to create and maintain a comprehensive asset inventory and data sets is an essential first step in incident response."**
>
> **— John Schneider, Senior Systems Engineer, Axonius Federal**

plethora of knowledge in a unified analytics space, and you don't have to go and actively collect it.

How can agencies improve cyber incident response?

Schneider The cybersecurity asset management segment is a very nascent space defined by Gartner only a few years ago.

The capabilities we are developing are essential in incident response because the amount of data agencies generate is growing exponentially. What they previously could manage with manual processes becomes unmanageable in today's scaled environment.

I think artificial intelligence (AI) is rapidly becoming a foundational piece of an incident response framework. AI is the next frontier when it comes to detection. AI could be a transformative technology in combing through the mountains of data, enabling incident responders and analysts to comb through the data and reduce response times.

But AI will only be as good as the model it is trained on.

AI will have the same problem as a cybersecurity analyst who is not given a complete and comprehensive data set. That's why investing in the right tools to create and maintain comprehensive data sets and an asset inventory overall is an essential first step in incident response.

Photo Credit: thinkhubstudio/Shutterstock

AXONIUS FEDERAL

WHY AXONIUS?

SEE AXONIUS FEDERAL IN ACTION

Schedule a demo with our team

info.axoniusfed.com/demo-request

GovCIO
MEDIA & RESEARCH

Cyber Incident Reporting Regulation Takes Shape

An upcoming CISA rule aims to harmonize cyber incident reporting requirements for critical infrastructure entities.

BY SILVIA OAKLAND AND AMY KLUBER

Photo Credit: Andrewshots/Shutterstock

Critical infrastructure entities in both public and private sectors are closer to getting a more comprehensive and coordinated approach to cyber incident reporting requirements with a new proposed rule from the Cybersecurity and Infrastructure Security Agency (CISA).

Currently open for public comment through June 3, 2024, the rule would require critical infrastructure organizations to report security incidents within 72 hours and ransomware payments within 24 hours. The rule comes amid an environment where agencies face what the Department of Homeland Security deemed "a patchwork of regulations and statutory authorities" that can often be competing or difficult to prioritize.

Federal agency strategies on cyber incident reporting largely have followed frameworks like those in CISA's Cybersecurity Incident and Vulnerability Response Playbook, which lists these steps:

- Preparation: Prepare for major incidents before they occur to mitigate any impact on the organization.
- Containment: Prevent further damage and reduce the immediate impact of the incident by removing the adversary's access.
- Education and Recovery: Allow the return of normal operations by eliminating artifacts of the incident and mitigating the vulnerabilities or other conditions that were exploited.
- Post-Incident Activities: Document the incident, inform agency leadership, harden the environment to prevent similar incidents and apply lessons learned to improve the handling of future incidents.
- Coordination: It is critical that the agency experiencing the incident and CISA coordinate early and often throughout the response process. It is also important to understand that some agencies have special authorities, expertise and information that are extremely beneficial during an incident.

CISA's playbook isn't the only resource critical infrastructure entities have in informing their reporting approaches. DHS outlines how duplicative and overburdened some of the current processes are in its September 2023 report on harmonizing cyber incident reporting measures.

Some agencies have approached it from a shared-services perspective. For example, the Department of Health and Human Services created a "one-stop cybersecurity shop" in its Administration for Strategic Preparedness and Response (ASPR) to help boost cyber resiliency in the health care sector.

CISA's upcoming rule when enacted will provide much-needed harmony to these approaches and streamline reporting protocol. For critical infrastructure entities, experts say this harmony will unlock more resources and time to devote to actually addressing a cyber incident.

"It will allow us to better understand the threats we face, spot adversary campaigns earlier, and take more coordinated action with our public and private sector partners in response to cyber threats," said CISA Director Jen Easterly in a statement. "We look forward to additional feedback from the critical infrastructure community as we move towards developing the final rule."

A Peek at GSA's Cyber Incident Reporting Plan

The General Services Administration aligns its cyber incident response plan to various directives including NIST Guidance 800-61R2, Computer Security Incident Handling Guide and CISA's playbook, according to GSA Security Operations Center and Incident Response Team Lead Eric Henry.

"GSA uses incident response playbooks and intelligent tooling to facilitate quick response actions," he told GovCIO Media & Research. "Preparation and lessons learned activities are the bedrock of quality response and continual improvement, both of which serve to provide better and quicker response."

GSA consolidates its cyber incident functions to feed into a security operations center at the agency.

(ctd.)

> “[The upcoming rule] will allow us to better understand the threats we face, spot adversary campaigns earlier, and take more coordinated action with our public and private sector partners in response to cyber threats.”

—Jen Easterly, Director, CISA

“It’s organized around the principle of enterprise shared service: ‘One GSA: One Cyber,’ ensuring a common approach including policy, process, team and tooling for incident response. … We ensure all information systems report into the SOC and use intelligent tooling for automated threat detection and focused detection and response,” said Henry. “Further, we have centralized and streamlined incident reporting and provide ongoing security awareness training to our staff focused on detecting and reporting incidents.”

Henry said a coordinated incident response plan is critical for agencies implementing emerging technologies like AI where it could also benefit cybersecurity approaches.

“GSA will invest in research and development to explore the potential benefits of implementing artificial intelligence in incident response, such as predictive analysis, machine learning and automation of certain tasks,” said Henry. “We will also build internal capabilities by training and upskilling employees in the use of artificial intelligence tools and technologies.”

Henry noted GSA’s cyber incident strategy will evolve as the agency learns from industry.

“We plan to collaborate with industry experts and partners to stay informed about the latest technologies and best practices in incident response,” said Henry. “GSA will also conduct regular evaluations and retros of current incident response processes to identify areas for improvement and streamline procedures.”

Photo Credit: Yuri A/Shutterstock