Agencies Accelerate Cyber Advances

govloop

Introduction

When it comes to cybersecurity, government agencies are playing the long game. Yes, cyber experts across the public sector continue to emphasize the importance of basic cyber hygiene practices, such as strong passwords, two-factor authentication, vulnerability management and so on. It's all necessary, but it's not sufficient.

Not when a new generation of hackers is tapping into a shadow market for hacking tools and services. Not when artificial intelligence (AI) is making existing tools and techniques more effective and devising new attack vectors. And certainly not when the rapid expansion of digital services is leaving agencies more vulnerable than ever.

Even as agencies at all levels of government look to shore up their existing cyber defenses, the federal government is working with partners across the public and private sectors to accelerate the development of innovative technology and practices. That is the focus of this report, the first installment of our three-part Cyber Guide series in 2025.

To lay the groundwork, we highlight quotable quotes from government experts discussing some of the big issues on the cyber agenda. The "Voices of the Community" section draws on GovLoop virtual trainings and roundtables, public events and key reports to capture a sentiment analysis, if you will, of the cyber community.

Next, we highlight government efforts to drive innovations around four key themes: AI, incident response, software bills of material (SBOMs) and the cyber workforce. In each area, we look at current efforts underway and what's to come. Collectively, these initiatives reflect the urgency that agencies feel as they seek to accelerate innovation.

Finally, we highlight the National Institute of Standards and Technology's (NIST) National Cybersecurity Center of Excellence (NCCoE), an ongoing effort to spur public-private collaboration on cyber advances.

We look forward to delving deeper into some of these issues in the coming installments of our Cyber Guide series.

Contents

3 Voices of the Community

5 Skills Benchmarking Lays the Groundwork for AI Success

6 The Future Is Now: Agencies Spur Cyber Innovations

- 7 AI Plays Defense
- 8 Incident Response Emphasizes Containment
- 9 SBOMs Take Shape
- 10 Cyber Workforce Development Expands

11 How NIST Fosters Deeper Engagement With Industry Partners

14 Further Reading

Voices of the Community

Sound bites that speak to top-of-mind issues in government cybersecurity

CYBER WORKFORCE

"Hiring managers aren't rushing to hire more specialized workers. Instead, they are prioritizing nontechnical skills like problem-solving that will be transferable through the increased use of AI."

2024 ISC2 Cybersecurity Workforce Study

INCIDENT RESPONSE

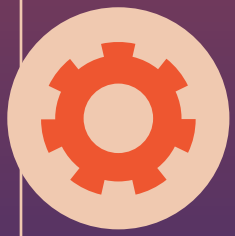
"We used to spend a lot of effort on [preventing attacks]. I think we have to shift a little bit and put more effort into [how we] respond and recover."

John Godfrey, Chief Information Security Officer (CISO), Kansas Information Security Office, speaking at a July 2024 virtual event

CRITICAL INFRASTRUCTURE

"Drinking water and wastewater systems are an attractive target for cyberattacks because they are a lifeline critical infrastructure sector but often lack the resources and technical capacity to adopt rigorous cybersecurity practices."

A March 2024 letter to governors from Environmental Protection Agency Administrator Michael Regan and Jake Sullivan, Assistant to the President for National Security Affairs



CYBER AWARENESS

"You may have 30 or 40 people in your security department, but you've got 2,000 or 10,000 employees. You need all those employees to [know] if they see something, they say something, so they're engaged and involved."

Michael Gregg, CISO, North Dakota, speaking at a June 2024 virtual event

COMPLIANCE

"From a compliance perspective, we know what the required security controls are. [What's needed is] a culture where we are consistently validating that security is working the way it intended."

Alvin "Tony" Plater, the Department of Navy's Acting CISO, speaking at a July 2024 virtual event

PHISHING

"We're still talking about phishing. The reason it persists is because it works. The cybercriminal groups are able to make money and advance their objectives."

Beau Houser, CISO, U.S. Census Bureau, speaking at a February 2024 virtual event

FUNDING

"While much work has been done by state and local governments to implement stronger cybersecurity protocols and address vulnerabilities, sustained federal funding is critical to ensure continued momentum."

A June 2024 open letter to Congress from state and local leaders

ARTIFICIAL INTELLIGENCE

"Overall, AI-enabled threats were the second most concerning form of cyberthreat, with 71% of CISOs characterizing AI threat levels as 'very high' or 'somewhat high.'"

2024 cybersecurity study from Deloitte and the National Association of State Chief Information Officers (NASCIO)

POST-QUANTUM ENCRYPTION

"Most actors are already using a 'store now and break later' framework, with the intention to decrypt it once they have the quantum capability."

Harry Coker Jr., National Cyber Director, speaking at the White House on Aug. 13, 2024

INDUSTRY SPOTLIGHT

Skills Benchmarking Lays the Groundwork for AI Success

> "There are a multitude of executive orders out there telling agencies they need to benchmark their skills. Agencies need to know where their starting line is and then make a plan based on the data."
>
> *– Tony Holmes, Pluralsight*

Cybersecurity has emerged as one of the top use cases for the new era of AI and generative AI (GenAI) solutions. As malicious actors turn to AI to make their attacks more lethal and difficult to detect, agencies need to use AI to augment their defenses.

The challenge is that they need to develop the workforce to support that vision. But workforce development involves more than just offering AI courses. It requires understanding the current skills gap and building a strategy for addressing it.

In this video interview, Tony Holmes, Practice Lead for Public Sector Solutions at Pluralsight, discusses how agencies can prepare their workforce for AI and other emerging technologies. Topics include:

→ Using benchmarks to shape your agency's training programs

→ Identifying employees who already have developed valuable GenAI skills

→ Helping the workforce see learning as a part of their jobs

ABOUT PLURALSIGHT

Pluralsight is the leading technology workforce development company that helps government agencies develop critical skills, improve processes and gain insights through data, and providing strategic skills consulting.

We help build technology skills at scale with expert-authored courses on today's most important technologies, including cybersecurity, cloud, AI, data science, and more. Our platform includes tools to align skill development with agency objectives, virtual instructor-led training, hands-on labs, skill assessments and one-of-a-kind analytics.

Learn more about Pluralsight

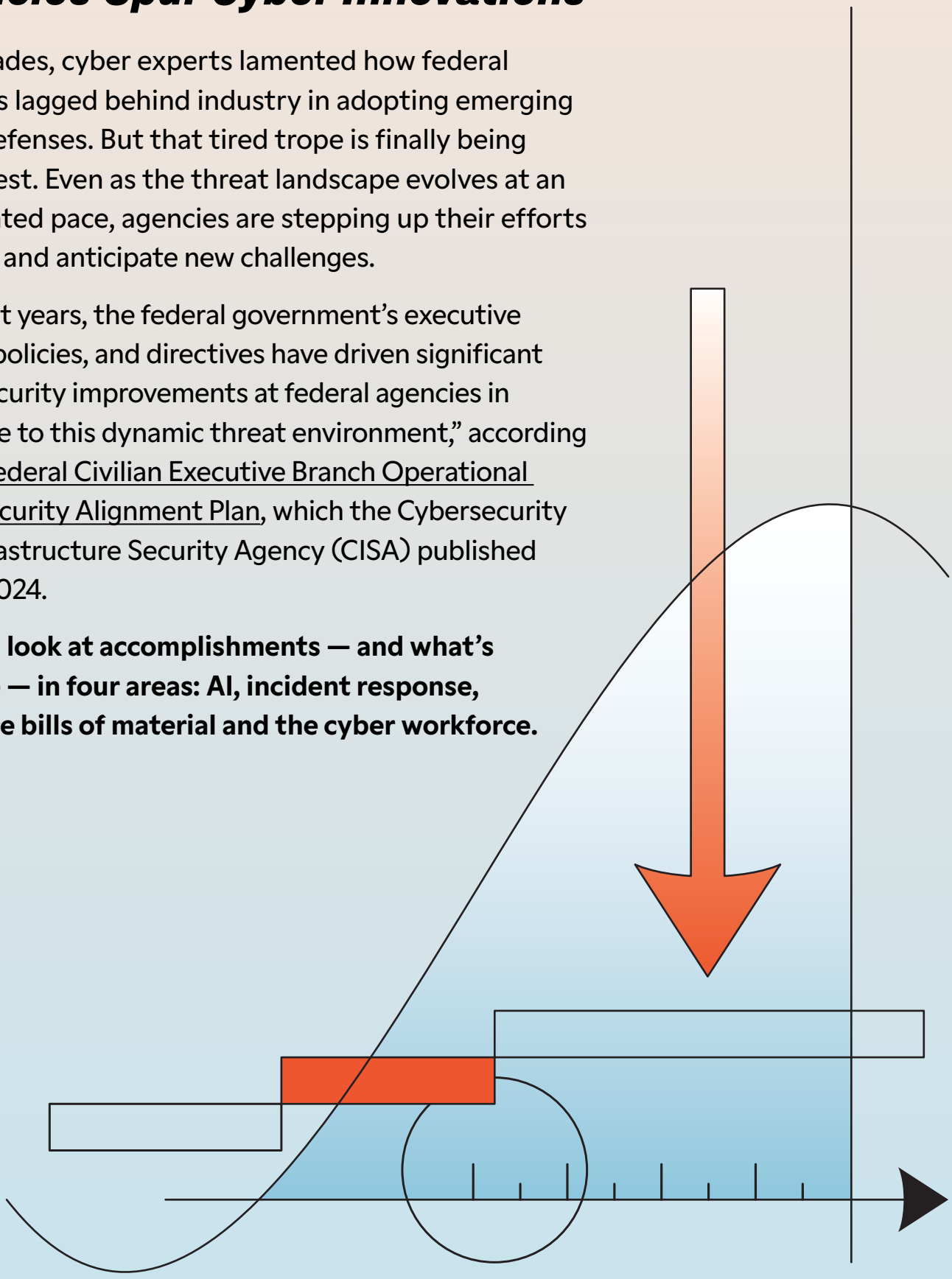
PLURALSIGHT | DLT

The Future Is Now: Agencies Spur Cyber Innovations

For decades, cyber experts lamented how federal agencies lagged behind industry in adopting emerging cyber defenses. But that tired trope is finally being put to rest. Even as the threat landscape evolves at an accelerated pace, agencies are stepping up their efforts to meet and anticipate new challenges.

"In recent years, the federal government's executive orders, policies, and directives have driven significant cybersecurity improvements at federal agencies in response to this dynamic threat environment," according to the Federal Civilian Executive Branch Operational Cybersecurity Alignment Plan, which the Cybersecurity and Infrastructure Security Agency (CISA) published in July 2024.

Here's a look at accomplishments — and what's to come — in four areas: AI, incident response, software bills of material and the cyber workforce.



AI PLAYS DEFENSE

Few technologies have taken off like AI; 64% of federal agencies use it almost daily, an August 2024 Ernst & Young report states. Although AI can strengthen cyber defenses, many people worry that it also strengthens malicious actors.

WHAT'S HAPPENING

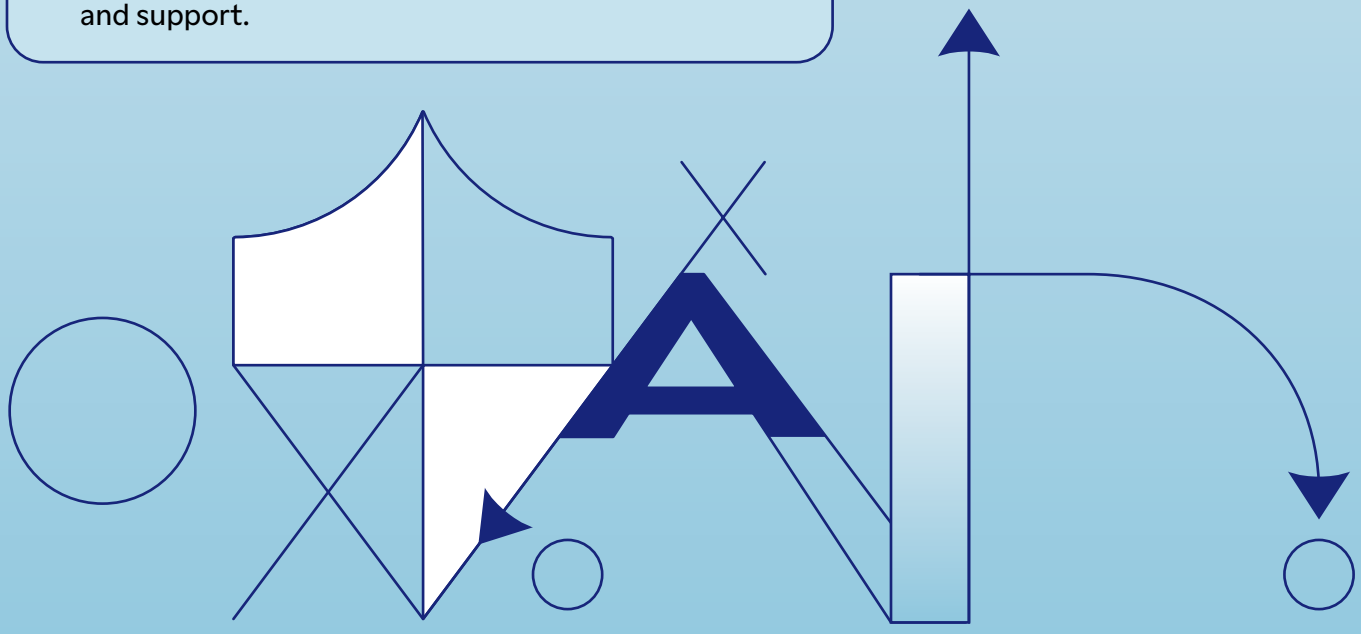
Several agencies are taking aim at AI to make sure it does more good than harm.

- → The National Science Foundation is sponsoring the **Institute for Agent-based Cyber Threat Intelligence and OperatioN** (ACTION), one of seven new National AI Research Institutes, to study the end-to-end cyber defense life cycle.
- → The Defense Advanced Research Projects Agency is hosting an **AI Cyber Challenge** in which competitors must "design novel AI systems to secure the open-source software that undergirds everything from financial systems to public utilities and the health care ecosystem." The final competition will be in August 2025.
- → The State Department released in May 2024 the **U.S. International Cyberspace & Digital Policy Strategy** with a focus on "digital solidarity," a concept of working with global partners to build cyber capacity and support.

WHAT'S COMING

The U.S. Cyberspace Solarium Commission published **10 AI-related recommendations** for the Trump administration and Congress. They include:

- → Prioritizing the protection of critical infrastructure
- → Codifying CISA's joint collaborative environment to facilitate real-time sharing and analysis of cyber threat intelligence
- → Boosting digital literacy among members of the public



INCIDENT RESPONSE EMPHASIZES CONTAINMENT

The National Institute of Standards and Technology (NIST) defines "incident response" as the "mitigation of violations of security policies and recommended practices," but it's about more than responding. A core component of NIST's Cybersecurity Framework, it includes reporting, or sharing incident information so that agencies can better anticipate and contain incidents.

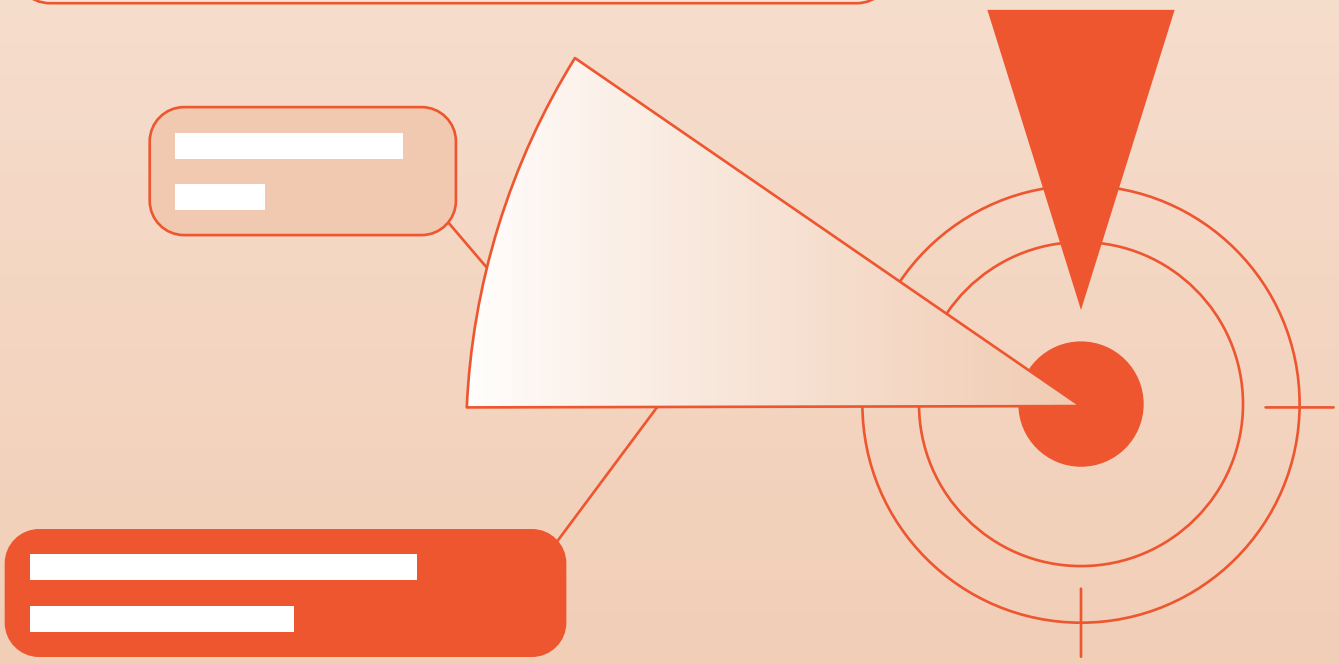
WHAT'S HAPPENING

Incident reporting is voluntary and, like most things cybersecurity, nuanced. Several agencies are working to bring some uniformity to the practice.

- → **CISA launched a secure portal** that can save, update, share, search and filter incident reports.
- → NIST released a draft revision to its **incident response special publication** that includes a new incident response life cycle model that separates preparation activities (governing, identifying and protecting) from response (detection, response and recovery).
- → Noting the health care industry's vulnerability to cyber risks — the number of large breaches increased by 93% between 2018 and 2022 — the **U.S. Department of Health and Human Services issued a cybersecurity strategy** to establish performance goals and incentivize sharing.

WHAT'S COMING

Look for a **new incident response and reporting rule** to come out of the U.S. Department of Homeland Security (DHS) in October 2025, a GAO report states. It's intended to improve the department's ability to coordinate federal cybersecurity and mitigation efforts and help entities defend against cyber incidents on critical infrastructure.



THE FUTURE IS NOW

SOFTWARE BILLS OF MATERIAL TAKE SHAPE

Known as SBOMs, these are lists of all the components in a software application. Although they're not new, SBOMs have found the spotlight because when they're incomplete, agencies can't know the true risk associated with the software.

WHAT'S HAPPENING

Although only 27% of software developers generate and review SBOMs now, according to research by ReversingLabs, more public and private entities are expected to require them. For instance, by 2025, 60% of organizations building or procuring critical infrastructure will require SBOMs, according to Gartner Hype Cycle for Open-Source Software. Some agencies are already moving in that direction.

- → In March 2024, CISA and the Office of Management and Budget released the **Secure Software Development Attestation Form** to provide a common way for "software producers who partner with the federal government [to] leverage minimum secure techniques and toolsets."
- → A **new Army memo** requires the service's procurement officers to incorporate SBOMs into most new contracts that involve software. The policy excludes cloud services.
- → The National Security Agency issued **Recommendations for SBOM Management**, outlining three steps: examine and manage risk, analyze vulnerabilities, and implement incident management.

WHAT'S COMING

CISA officials are working hard to simplify the complex task of itemizing software components. Look for more guidance to come out similar to the third edition of "**Framing Software Component Transparency: Establishing a Common Software Bill of Materials**" that CISA published in September 2024.

THE FUTURE IS NOW

CYBER WORKFORCE DEVELOPMENT EXPANDS

Cybersecurity workers are often the first line of protection and defense — a job made that much harder by the speed of innovation, slow procurement processes and employees who flaunt IT rules. A problem across all government levels, it's especially troublesome for state and local agencies.

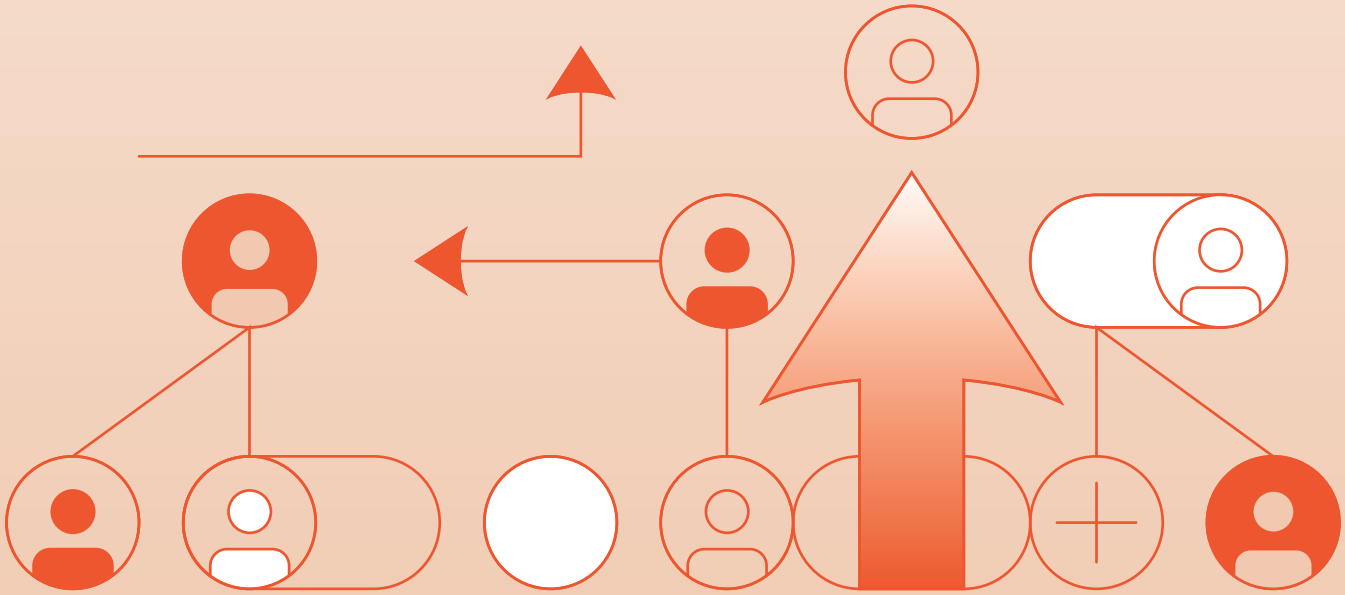
WHAT'S HAPPENING

Cyber workers can earn six-figure salaries, according to the Bureau of Labor Statistics, yet there's a global shortage of more than 4 million cyber professionals, the World Economic Forum states. Governments are trying to recruit more people in the field — and to train current employees to be more cyber-literate.

- → Agencies including NIST and the Labor Department received **millions of dollars in grants** in 2024 to develop their cyber workforces.
- → NASCIO labeled **expanding and strengthening the state cyber workforce** a top priority for 2024, citing challenges such as attrition and wage competition, namely with the private sector.
- → The SANS Institute emphasizes **quality over quantity**: "To keep up with changing threats...cybersecurity teams need to be more proactive with their skills, not just larger in terms of headcount."

WHAT'S COMING

Proposed legislation is floating through Congress to bolster the cyber workforce. One bill would establish a **full-scholarship, CISA-run program** for two-year degrees at community colleges and technical schools in exchange for government service. Another, the **Federal Cyber Workforce Training Act of 2024**, would create a central training center for cyber workforce development.



How NIST Fosters Deeper Engagement With Industry Partners

An interview with Cheri Pascoe, Director of the National Cybersecurity Center of Excellence (NCCoE) at the NIST

In theory, cybersecurity experts widely agree that public/private partnerships make perfect sense. But in practice, they are often less certain about how to make them happen: How do you engage with technology firms outside of individual projects? How do you structure a partnership that results in concrete advances in technology and tactics? How do you balance the different needs of both government and industry participants?

NCCoE has been wrestling with those kinds of questions since it was established in 2012. The center works with industry, government agencies, academia and other organizations to tackle the country's most pressing cybersecurity challenges.

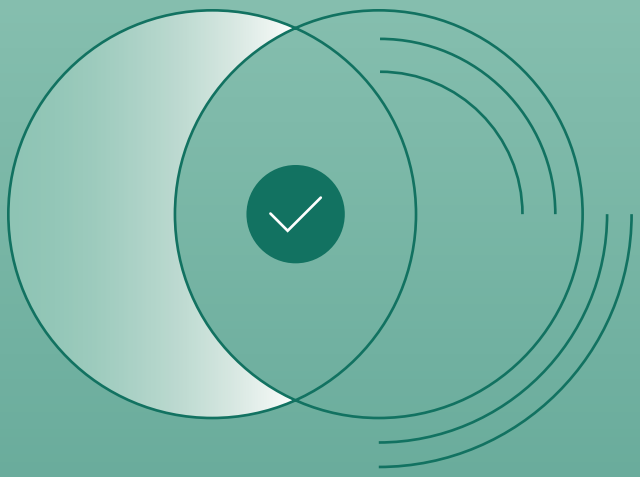
NIST, which has been doing cybersecurity research and standards development for more than 50 years, has always collaborated with other organizations, said NCCoE's Cheri Pascoe. "We wanted, however, to more deeply engage with industry and other government agencies to apply some of the work that NIST has been doing," she said. "In some respects, we view the NCCoE as an entity to transition standards into practice."

A FOCUS ON BIG CHALLENGES

Pascoe said NCCoE operates something like an applied research laboratory. The center builds cross-sector teams with external collaborators that tackle specific cybersecurity challenges by leveraging commercially available technology and existing cybersecurity standards and best practices. Currently, focus areas include:

- → **Post-quantum cryptography.** NCCoE is developing guidance for adopting new cryptography standards that quantum computers can't break.
- → **Critical infrastructure resilience.** The center is looking at how to tailor cybersecurity solutions and practices to specific sectors, including energy, health care and space. Most recently, it launched a project on water utilities' cybersecurity, which has become a major concern in the past year.
- → **Digital identities.** A growing number of states are looking to adopt mobile driver's licenses, which can be stored, managed and updated on mobile devices. NCCoE is working on a basic architecture for the technology and processes and developing possible use cases.

"These are areas where we have the ability to work closer with the [stakeholders] and really try to understand their specific cybersecurity challenges, and how certain technologies might be able to be leveraged to address them," Pascoe said.



AN EMPHASIS ON LISTENING

Beyond specific projects, NCCoE looks to technology companies to provide insight into cybersecurity trends, both in terms of the challenges their customers are facing and the emerging solutions.

Thirty-nine firms have signed memorandums of understanding with the center, allowing them to serve as partners that meet with NCCoE representatives on a quarterly basis. Most are very large technology vendors that have a vested interest in understanding the changing cybersecurity landscape, Pascoe said.

"We do a lot of listening, trying to learn where there might be common challenges popping up in different communities, and then once we have a topic identified, [we] try to align that topic with the expertise of NIST," she said.

Often, the center early on organizes virtual or in-person meetings so that it can increase awareness and provide potential collaborators with more insight into a project's direction. But even that becomes another opportunity to get feedback, she said.

CULTIVATING A SHARED COMMITMENT

This deeper level of engagement requires a sense of shared commitment that looks beyond any immediate return on investment of time and resources, Pascoe said. To make it work, both parties must recognize the longer-term benefits.

For NIST, the benefits are straightforward. It gains access to the technical expertise and market insights of leaders in the field. Through these engagements, it also can influence the development of solutions.

For technology firms, which are assessed, in large part, on financial returns, the benefits are more nuanced, Pascoe said. NIST recognizes that people working on these projects might otherwise be building or selling products with a more direct impact on the bottom line, Pascoe said.

But the benefits can be substantial, nonetheless. It's important to work with potential collaborators to help them articulate the value and get buy-in from their leaders, she said. Possible advantages include:

- → Vendors better understanding, through a project, how their products might be used and what improvements they might want to make to a product or product line
- → Participants highlighting their collaboration with NIST
- → Participants tapping into the broader cyber community's expertise and bringing that back to their firms

GOOD COMMUNICATIONS FROM START TO FINISH

Once selected, a project develops in three steps: defining the work, assembling a team and building the solution (see sidebar). Strong communications are essential throughout the process, Pascoe said.

Early on, it's essential to create awareness around the project, beyond just publishing its description in the Federal Register. Even vendors that NCCoE has worked with numerous times could miss that notice and subsequent announcements about workshops.

"People are overwhelmed," Pascoe said. "There's so much going on in the world that you have to constantly communicate with potential collaborators to be able to get them onto a project."

And once on a project, leaders maintain a regular cadence of communications, meeting with the full consortium either once a week or every two weeks to update them on timelines and activities. "We also are looking for ways to just keep people informed even if they aren't personally involved at a given time," she said.

One of the challenges, however, is the high rate of employee turnover in the cybersecurity field. In some cases, NCCoE was working with one person from a company and suddenly that person was gone. To avoid having single points of failure, the center tries to keep in touch with a broader range of contacts, she said, and create more of an institutional level of engagement.

The payoff of building and maintaining a high level of engagement is clear, Pascoe said. "It's really a beautiful thing to see the improvements that we're able to make to cybersecurity – the way that we're able to bring different experts together that wouldn't normally work together to solve these cybersecurity challenges," she said.

HOW NCCOE WORKS

Once NCCoE has decided to take on a project, it follows a three-part process:

1. DEFINE

NCCoE subject-matter experts draft a project description that defines the challenge and then release it for public comment. Once they've gotten feedback, they finalize the description along with a draft architecture for a possible solution.

2. ASSEMBLE

NCCoE invites organizations from government, industry and academia to submit letters of interest, with organizations accepted on a first-come basis. Collaborators on the project provide in-kind contributions of technology (hardware, software, services) and people (expertise). All organizations sign a cooperative research and development agreement, which provides legal guardrails for sharing information and technology.

3. BUILD

The reference architecture is finalized, and the various organizations work with NCCoE to translate that architecture into a working solution. Teams typically meet weekly for the life of a project, which can run several years.

Dig Deeper: Recommended Reading

One guide can only capture so much. Here are some of the key resources touched on throughout this report, so you can learn more.

Top 10 Recommendations for the Incoming Administration and Congress

The Cyberspace Solarium Commission, which was created by Congress in 2019, originally provided a list of more than 50 recommendations for improving the nation's cyber capabilities. The group's 2024 report on implementation flags 10 priorities for follow-through by the new administration.

The Federal Civilian Executive Branch (FCEB) Operational Cybersecurity Alignment Plan

CISA highlights proven practices in the full cyber life cycle, from prevention to incident detection and response, and identifies overarching cybersecurity goals that can apply to a wide range of agencies.

Leveraging AI to Enhance the Nation's Cybersecurity

The DHS Science and Technology Directorate is exploring a number of cyber use cases for AI and machine learning.

Incident Response Recommendations and Considerations for Cybersecurity Risk Management (Rev. 3)

This document, still in draft, is intended to help organizations incorporate incident response tactics throughout the cybersecurity risk management activities laid out by NIST's Cybersecurity Framework 2.0.

Framing Software Component Transparency (2024)

This third edition of CISA's guidance describes the key elements of a software bill of materials that can be applied to all software and offers recommended practices and "aspirational goals."

govloop

Preregister for the next installments of GovLoop's 2025 Cyber Guide Series

govloop.com
@govloop