

SECURING DATA Against Evolving CYBER THREATS

INSIDE:

Inside Trump's Cyber Executive Order	3
Infographic: Post-Quantum Cryptography	6
DOD's Evolving Cyber Strategy	11

SPONSORED BY



From the editor's desk



Sarah Sybert, Managing Editor

Protecting Data in the Next Cyber Era

The next era of cybersecurity is defined by speed, complexity and value of data. Adversaries are leveraging AI and automation to move faster, targeting credentials and exploiting hybrid infrastructures that stretch far beyond traditional perimeters.

Federal agencies are pivoting data security strategies and adopting new approaches like zero trust and cloud-native defenses to align with President Donald Trump's cyber executive order and secure information against evolving threats. The order refocuses investments on encryption, supply chain security and international cyber cooperation.

Inside, you'll learn how leaders from the War Department, CDW

Government and the White House are confronting data security head on. DOW Cyber Chief David McKeown explains how the agency is modernizing its cryptographic infrastructure, accelerating software security through automation and driving toward full zero trust adoption by 2027.

Meanwhile, CDW Public Sector Field CISO Steve Thamasett details how cloud platforms, automation and workforce training are helping agencies regain visibility and keep pace with AI-enabled threats.

The next cyber era will require IT officials to develop the right tools, culture and strategy to effectively secure data. 🌟

Table of Contents



Ross Gianfortune,
Senior Staff Writer

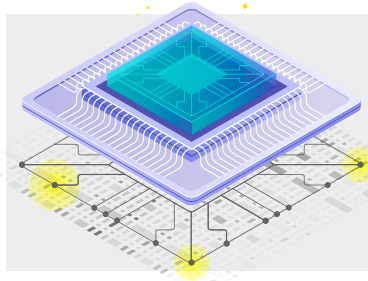


ARTICLE

Trump Overhauls Federal Cybersecurity with New Executive Order

The new directive aims to strengthen digital defenses while rolling back “burdensome” software requirements and refocusing AI security.

BY ROSS GIANFORTUNE



INFOGRAPHIC

Preparing for a Post-Quantum Future

Quantum computers threaten to break the encryption securing federal systems, making post-quantum cryptography critical for protecting national security.



PARTNER INTERVIEW

Meeting the Evolving Challenges of Data Security

Federal agencies need to shift data security strategies and adopt new approaches to secure against future threats.

Steve Thamasett, Public Sector Field CISO, CDW Government



ARTICLE

Pentagon Cyber Strategy to Adapt to New Budgets, Tech Innovation

Budgetary pressures spur innovation as War Department tackles aging infrastructure and evolving threats, says top cyber official.

BY ROSS GIANFORTUNE

Trump Overhauls Federal Cybersecurity with New Executive Order

The directive aims to strengthen digital defenses while rolling back “burdensome” software requirements and refocusing AI security.

BY ROSS GIANFORTUNE

President Donald Trump signed an executive order in June aimed at strengthening cybersecurity. According to the White House, the order promotes the development of secure software, encourages the adoption of the latest encryption protocols and further secures internet routing.

The order, titled “Sustaining Select Efforts to Strengthen the Nation’s Cybersecurity and Amending Executive Order 13694 and Executive Order 14144,” directly targets and modifies key provisions from cybersecurity directives issued by both the Biden and Obama administrations. According to a White House fact sheet, the order also seeks to amend “problematic elements” of Biden administration orders, including “unproven and burdensome software accounting processes” and “micromanaged technical cybersecurity decisions.”

The new order explicitly removes provisions that would require federal contractors to submit “secure software development attestations” and accompanying technical data. It also eliminates requirements for the Cybersecurity and Infrastructure Security Agency to verify these attestations and for the Office of the National Cyber Director to publish review results.

The White House justified these changes by stating that such measures prioritized “compliance checklists over genuine security investments.”



“President Trump has made it clear that this administration will do what it takes to make America cyber secure — including focusing relentlessly on technical and organizational professionalism to improve the security and resilience of the nation’s information systems and networks,” a White House fact sheet reads. (ctd.)

The executive order emphasizes several critical areas:

- **Enhanced Cybersecurity Standards:** Agencies are directed to update their cybersecurity frameworks, prioritize zero-trust architectures and implement advanced threat detection systems. This builds upon the Biden administration's January order's mandates but accelerates adoption through dedicated funding and technical support.
- **Supply Chain Security:** The order underscores the importance of scrutinizing and securing supply chains, especially for software and hardware components. It mandates stricter vetting processes for suppliers and incentives for developing secure, trusted technology ecosystems.
- **Incident Response and Resilience:** Recognizing the growing sophistication of cyber adversaries, the order calls for improved incident response protocols, regular cyber drills and increased transparency around cyber incidents affecting federal operations.
- **International Cooperation:** Cyber threats often breach borders, and the executive order highlights the need for stronger international cooperation, information sharing and joint capacity- building initiatives aimed at combating transnational cybercriminal networks.
- **Workforce Development:** To sustain long-term resilience, the Biden administration emphasizes expanding cybersecurity workforce training programs, fostering public awareness and encouraging innovation in cybersecurity technologies.

(ctd.)



“President Trump has made it clear that this administration will do what it takes to make America cyber secure.”

— White House

The order also streamlines post-quantum cryptography (PQC) and artificial intelligence cybersecurity initiatives. The order “refocuses AI cybersecurity efforts towards identifying and managing vulnerabilities, rather than censorship,” and requires a regularly updated list of product categories that support PQC.

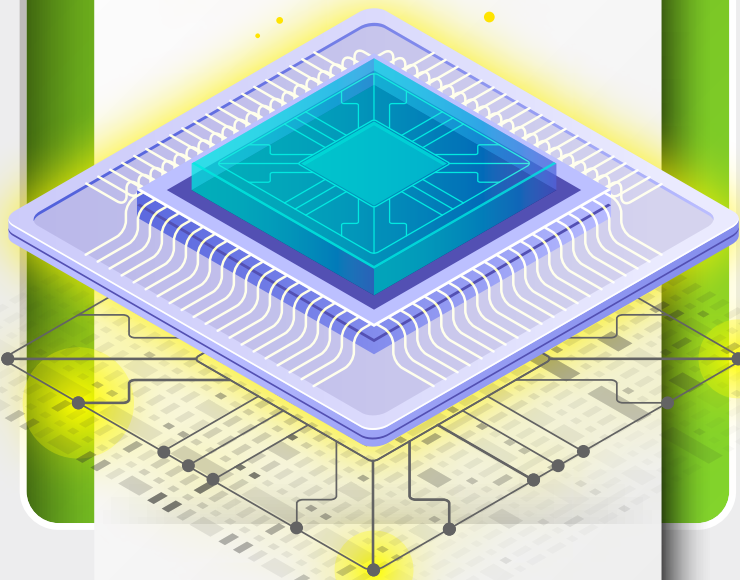
“President Trump has already taken action to remove barriers to AI innovation, ensuring that our technology sector remains competitive at the cutting edge of new developments and free from ideological bias,” reads the White House fact sheet. 🌸

Preparing for a Post-Quantum Future

Quantum computers threaten to break the encryption securing federal systems, making post-quantum cryptography critical for protecting national security.

THE QUANTUM THREAT

Quantum computers are being developed to solve problems that are too complex for today's machines, like drug design and molecular simulations. But this same power poses a major security risk: once they are powerful enough, quantum computers could break the encryption that protects everything from personal banking to national security data.



WHY CURRENT ENCRYPTION IS VULNERABLE

Today's encryption relies on the difficulty of factoring very large prime numbers. Conventional computers would need billions of years to solve this puzzle, making current encryption secure. However, quantum computers could try all possibilities at once, reducing the time needed to break encryption from millennia to just days or hours. This makes sensitive data, even if stolen today, vulnerable to future attacks.



POST-QUANTUM SOLUTIONS

To stay ahead of the threat, researchers are developing new encryption methods known as post-quantum cryptography (PQC). These algorithms are designed to resist both classical and quantum attacks. The National Institute of Standards and Technology (NIST) has already finalized the first set of standards, built on mathematical problems that are far more difficult for quantum computers to solve. By adopting these new algorithms now, organizations can protect data against the powerful quantum computers of tomorrow.





Meeting the Evolving Challenges of Data Security

Federal agencies need to shift data security strategies and adopt new approaches to secure against future threats.

What are the challenges of data security?

Thamasett Historically, agency data resided primarily in on-premises data centers, offering a manageable and observable environment. Agencies could monitor their systems effectively and respond to threats in real-time. However, the shift toward hybrid infrastructures has significantly complicated this picture. Today's networks include diverse components such as sensors, internet of things (IoT) devices and many IP-enabled endpoints, leading to reduced visibility across the entire environment.

This diminished visibility presents a core challenge: many seemingly innocuous activities, when correlated across different parts of the network, can reveal malicious intent. The ability to detect these subtle indicators is now more critical than ever, with organizations striving to integrate advanced monitoring capabilities that can connect the dots seamlessly.

The volume of data generated and the rapid speed at which this data expands compounds these complexities. Agency data



Steve Thamasett
Public Sector Field CISO,
CDW Government

remains the paramount asset — its protection is vital — and it continues to be the primary target for adversaries. Attackers are becoming more sophisticated, employing AI not only to find vulnerabilities but to mimic trusted identities through credential targeting. Even organizations with robust policies and procedures face risks when attackers compromise credentials, granting them access to sensitive data despite preventive measures.

What are some of the successes or use cases for technology you've seen helping?

Thamasett Amid these challenges, innovative technological initiatives are delivering tangible benefits. The push toward zero-trust architectures, which emphasize strict identity verification and least privilege access, has led many

agencies to adopt multi-factor authentication (MFA) more broadly. Secure cloud adoption has also emerged as a vital element — initial cloud migration was often rushed without fully understanding security implications, but current practices involve selecting FedRAMP-certified cloud providers tailored to specific impact levels to ensure compliance and security.

Cloud-based security tools have played a pivotal role by restoring visibility that is lost with the transition away from traditional network perimeters. These platforms enable agencies to enforce policies uniformly, monitor access comprehensively and respond swiftly to potential threats.

Workforce development has become another cornerstone of effective data security. Recognizing that security is a collective responsibility, agencies are fostering a security-aware culture. Initiatives such as internal phishing

“Automating the security operations center (SOC) with the same kind of ML and AI that the bad actors are using is critically important. The attacks have gotten faster, exfiltration has gotten faster, so your reaction time must be faster.”

— Steve Thamasett, Public Sector Field CISO, CDW Government



simulations educate employees, turning them into active defenders. Cloud environments facilitate the consolidation of data and identity stores, simplifying security management and enforcement.

What are some of the emerging solutions in this space?


Thamasett Looking ahead, several emerging solutions promise to strengthen data security further. Automation of security operations centers (SOCs) through machine learning and artificial intelligence is crucial. Advanced tools capable of correlating events rapidly effectively augment human analysts, allowing for faster, more accurate responses.

Automating the SOC with the same kind of ML and AI that the bad actors are using is critically important. The attacks have gotten faster, exfiltration has gotten faster, so your reaction time must be faster.

Cloud security platforms are also evolving to provide comprehensive visibility, enabling organizations to understand their environment from an attacker's perspective. This insight is critical for preemptive defense and

incident response.

Innovative technologies such as blockchain are poised to revolutionize information sharing within secure supply chains, providing tamper-proof records that enhance trust and authenticity. Additionally, the rapid development of quantum computing presents both a threat and an opportunity: as quantum's immense processing power threatens to break current encryption standards, the emergence of quantum-resistant cryptography becomes essential. Staying ahead of this curve is vital to maintain long-term data security.

As threats continue to evolve in complexity and speed, so must the strategies and technologies used to defend against them. From advanced, AI-driven security automation to the emerging threat of quantum computing, the future of data security hinges on innovation, collaboration and proactive adaptation. By harnessing the latest in security tools and cultivating a security-aware organizational culture, agencies can better position themselves to meet these ongoing challenges head on. 



An era of evolution

Meeting your needs. Every step of the way.

Strategic, intentional acquisitions

Collaboration on any initiative

Never get stuck on a challenge, continue the mission.

- Talent orchestration services
- Digital Government
- IT Modernization
- Digital Tools
- Cybersecurity
- AI

Services ready to meet you where you're at

We are ready to join you at any stage, on any journey.

- Managed services
- Data governance
- Cybersecurity
- Infrastructure management
- Cloud-cost optimization

Specialized knowledge you can trust

You've got it? We've seen it — and can make it work harder for you.

- ServiceNow
- IT asset management
- Government digital experience



CDW Government

Pentagon Cyber Strategy to Adapt to New Budgets, Tech Innovation

Budgetary pressures spur innovation as the War Department tackles aging infrastructure and evolving threats, says top cyber official.

BY ROSS GIANFORTUNE

The War Department is entering a significant phase of rationalization and innovation in its cybersecurity strategy, driven by budgetary constraints and an evolving threat landscape, officials explained at an industry event earlier this year.

“We’re kind of in a heavy rationalization phase right now and exploring all of the ideas that we can to do things better and faster,” said David McKeown, CIO’s special assistant for cybersecurity innovation at DOW. “It’s not just traditional IT networks, it’s weapon systems, it’s critical infrastructure. And it’s working with the defense industrial base on their cybersecurity as they do work with us.”

McKeown outlined initiatives aimed at bolstering the department’s defenses, streamlining processes and fostering stronger partnerships with industry. Quoting Winston Churchill, “All right, everybody, we’re out of money. Now we have to start thinking,” he said, adding that DOW needs to innovate its cybersecurity positioning under budgetary constraints.

“We’re kind of in the thinking phase of reinventing how we do a lot of things. In the department, we’ve been allowed to grow work on processes, some of them bureaucratic, some of them not,” said McKeown. “Some of them needed. Some of them not.”



Encryption as a Top Priority

McKeown said encryption is the new number one priority. The aging cryptographic infrastructure currently in place across various DOW platforms is increasingly vulnerable to advanced adversaries and the looming threat of quantum computing.

“For many years, we relied on [cryptography] on all of our different



**David
McKeown**

**CIO's Special Assistant for
Cybersecurity Innovation, DOW**

platforms,” said McKeown. “It’s getting old. The algorithms are getting old. The architectures are getting old. Our adversaries are getting more advanced. The advent of quantum is making progress, and we’ve got to be worried about that as we go forward.”

McKeown said that a key element of cryptographic modernization involves addressing the vulnerabilities associated with public key infrastructure (PKI) in a post-quantum world. He noted that DOW hired Dr. Britta Hale to lead a centralized and orchestrated effort to identify and replace PKI algorithms across DOW’s software landscape with quantum-resistant cryptography.

“As we look at quantum and that problem set, we have to rationalize all of our software and find out where PKI is used and go in there and change the algorithm,” said McKeown.

DOW’s Risk Management Strategy

McKeown said that DOW is working to fix the risk management framework (RMF) at the department. The older RMF process, a compliance-driven model, is increasingly viewed as inadequate for real-time cybersecurity needs. McKeown said that DOW is working together to automate RMF functions, eliminating human error, expediting assessments and reducing costs.

The department is exploring automation tools, continuous monitoring, enterprise inheritance of controls and cloud service provider integrations within the RMF structure, McKeown said. The goal, he added, is to streamline the RMF to include security controls, reduce redundant paperwork and establish clearer communication channels between system owners, cybersecurity service providers and authorizing officials.

“What we found, though, is RMF is a compliance drill,” said McKeown. “It is not achieving cybersecurity the way we want it.”

(ctd.)

Bolstering Zero Trust

DOD is committed to zero trust adoption throughout the department with the 2027 goal as a mile marker. Progress includes near-complete certification of Navy's Flank Speed, Defense Information Systems Agency's Thunderdome environments, McKeown said.

"By 2027, we'll have built a series of minefields throughout the Department of Defense that the adversary, if they wander into one environment that is zero trust, chances are that we'll catch them and be able to use that intelligence to inform others [of the threat]," said McKeown.

Software Fast Track

McKeown said the recently-announced DOD Software Fast Track (SWFT) program seeks to define strict industry criteria — such as software bill of materials and secure development frameworks — and streamline certification processes, accelerating the deployment of secure, mission-ready software. In a tighter budget environment, he said, DOD's software deployment and acquisition programs need to become more cost-effective and useful.

"I don't think we've done software security or supply chain risk management on software very well to date," McKeown added. "The idea here is define criteria that we tell industry that they need to meet."

Weapons Systems Cybersecurity Controls

Addressing concerns about potential budget cuts, McKeown called on the military services to take on a greater role in weapon system cybersecurity analysis. With more than 200 key weapon systems, McKeown said that DOD intends to empower service branches to conduct risk assessments, enabling faster and more effective defensive measures.

The DOD will also focus on developing better assessments for combat commands to better understand the mission impacts of cyber risks identified in



their systems, he said.

“We’re also working on scorecards for the combat commands they need to know the risks that they’re incurring across all of those systems,” said McKeown.

“We do an analysis of a weapon system, and we publish it, but I don’t think the combat commands really understand the impacts of their mission.”

AI and the Future of Cybersecurity

The DOW is also actively exploring the secure integration of artificial intelligence for

both offensive and defensive cyber operations, McKeown said. The department needs to keep its data within its boundaries for security, while empowering the DOW workforce to use AI in their everyday work.

“We’ve got to train a workforce that is capable of doing all the things that you need to do in AI, defense, offense, just normal, optimizing your work so that you can do it better in leveraging AI,” said McKeown. “We’re not sticking our head in the sand. We’re embracing it.” ✨

“The algorithms are getting old. The architectures are getting old. Our adversaries are getting more advanced. The advent of quantum is making progress, and we’ve got to be worried about that as we go forward.”

**—David McKeown, CIO’s Special Assistant
for Cybersecurity Innovation, DOW**