veeam

What the Cyber Strategy for America Means for Federal Cyber Resilience

As cyber threats grow more disruptive, the Cyber Strategy for America calls on federal agencies to strengthen resilience, protect mission-critical data, and prepare for faster recovery.

Federal agencies are operating in a more aggressive, coordinated, and persistent threat environment than at any point in recent history. Cyber incidents are no longer isolated disruptions. Instead, they have grown into operational events capable of halting missions, disrupting essential services, and undermining public trust.

In response to the evolving threat landscape, the White House released the Cyber Strategy for America, outlining a framework to strengthen national cyber defense by improving coordination, resilience, and response to cyber threats. Organized around six pillars, the strategy emphasizes deterrence, modernization, infrastructure protection, technological leadership, and workforce development.

For federal leaders, the strategy reflects an important evolution in cybersecurity thinking. Preventing attacks is essential, but resilience is just as important.

"Not treating cyber incidents as unlikely events that we just try to prevent is critical," said James Walsh, senior director of government strategy for Veeam. "Acknowledging that recovery is essential to ensuring that federal agencies can get up and running as quickly as possible is a big part of the strategy."

Across the strategy's six pillars, the ability to protect and recover mission-critical data proves to be increasingly central to federal cyber preparedness.

Pillar 1: Shape Adversary Behavior

The strategy's first pillar focuses on bolstering deterrence and the government's focus and ability to orchestrate disabling cyber adversaries before they can disrupt systems. This includes using law enforcement, intelligence, and cyber operations to dismantle malicious networks and raise the barriers to entry for attackers.

To use an example, ransomware attacks depend on the inability of victims to quickly restore their data or systems. When organizations have the correct technology, people, and processes in place to demonstrate the ability to recover operations rapidly, attackers lose much of the leverage that makes these attacks profitable.

Working through public-private collaboration to ensure reliable recovery capabilities are in place can therefore be one of the most practical ways organizations, including federal agencies, reduce the impact of cyberattacks and disincentivize bad actors.

Pillar 2: Promote Common-Sense Regulation

The second pillar calls for clearer cybersecurity requirements for the industry. Federal leaders are pushing for standards and rules that streamline security compliance burdens across critical systems and technology providers.

It is likely that future regulation will only increase the focus on visibility and timely incident reporting. Companies must be able to determine what systems were affected during an incident, what data may have been exposed, and how long attackers were present.

"It's very difficult to meet reporting requirements unless you have both the people and sophisticated systems in place to track what got hit, what data might have been affected, and how long an attacker was in your environment," said Jeff Reichard, vice president of solution strategy at Veeam.

As cybersecurity policies evolve, the ability to quickly assess and report the scope of incidents will become an increasingly important operational capability.

Pillar 3: Modernize and Secure Federal Government Networks

The third pillar emphasizes modernizing federal technology infrastructure as a core component of strengthening the nation's cybersecurity posture. The strategy encourages agencies to accelerate adoption of zero trust architectures, cloud services, and post-quantum cryptography to build more secure, resilient environments.

"It's critical to de-risk the migration and modernization process by taking the right steps up front," Reichard said. "Agencies need to understand what data they actually need to move to bring new services online, and stakeholders need assurance that data in the cloud or new service will be at least as secure, available, and scalable as it was in legacy systems."

Modernization also changes the scale of cyber recovery. Mission systems and data are now distributed across hybrid environments that include on-premises infrastructure, cloud platforms, and software-as-a-service applications, and feed into the deployment of emerging tools like artificial intelligence platforms.

As agencies urgently modernize their environments, recovery planning must evolve alongside those architectures.

Pillar 4: Secure Critical Infrastructure

The fourth pillar emphasizes the importance of protecting the critical infrastructure systems that underpin daily life in the United States — from energy grids and financial networks to hospitals and water systems. Because these services often span federal agencies, private operators, and state and local governments, they have become attractive targets for cyber adversaries seeking to disrupt operations or create widespread instability.

That complexity can make recovery planning difficult, but even more critical.

"When we go through Data Resilience Maturity Model exercises with the public and private sector, they are almost always surprised by gaps that they did not know that they had," Reichard said, emphasizing the importance of regularly testing backup and recovery processes.

Across the country, state and local governments are already working to strengthen resilience around critical services. In Birmingham, Alabama, IT leaders worked with Veeam to modernize their backup and recovery environment, and ensure systems supporting police records, emergency services, and city operations are restored quickly during disruptions. The effort strengthened Birmingham's business continuity and disaster recovery strategy while saving the city more than $100,000 in IT costs and staff time.

Pillar 5: Sustain Superiority in Critical and Emerging Technologies

The fifth pillar centers on sustaining U.S. advantage in critical and emerging technologies by securing the data, infrastructure, and systems that support them. It emphasizes building security into technologies and supply chains from the outset, advancing protections such as post-quantum cryptography, and safeguarding the full AI technology stack. Veeam believes a core focus on protecting data is essential to maintaining trust in these systems.

"For the last decade we've dealt with cyber resiliency where malicious actors encrypt data or attack entire data centers," Reichard said. "AI resilience is the next evolution, where the scope of what you need to recover can include AI agents, models, and the data used to train them."

AI systems rely on curated data and trained models that power critical insights and automation. Ensuring those assets are protected and recoverable allows agencies to adopt AI capabilities across mission environments with greater confidence and continuity.

Pillar 6: Build Cyber Talent and Capacity

The strategy's final pillar emphasizes strengthening the nation's cyber workforce and expanding collaboration across government, industry, and academia. Building that capacity is essential to ensuring agencies and the nation can respond to incidents effectively and sustain operations in the face of disruption.

Developing the next generation of cyber professionals will require closer alignment between academic institutions, employers, and real-world mission needs. Programs that provide hands-on experience and exposure to operational environments help prepare students to support critical functions such as data protection, recovery, and resilience.

At Veeam, investments in talent development and university relationships are designed to help expand this pipeline, especially through engagement with institutions across the United States — such as Carnegie Mellon, Georgia Tech, Purdue, and the University of Maryland, as well as regional schools and HBCUs. By creating opportunities for students to gain practical experience, these efforts support broader workforce readiness while reinforcing the capabilities organizations need to resource their cybersecurity priorities.

Turning Strategy Into Operational Resilience

The Cyber Strategy for America reflects a broader shift in how the United States approaches cyber defense. Preventing attacks remains essential, but agencies must also ensure they can restore systems and data quickly when incidents occur.

Building that level of resilience requires not only stronger internal capabilities but also close collaboration between government and industry.

"There's a reason why there's a big focus on collaboration from the government perspective," added Reichard. "It allows faster innovation. Anything we can do to further that from the industry side is going to be better for all of us."

Solutions designed for data resilience, such as Veeam's secure backup, recovery, and data protection capabilities support that mission. By maintaining immutable backups, verifying recovery points, and restoring systems across hybrid environments, agencies can reduce operational downtime and limit the impact of cyber incidents.

"Looking ahead, we are energized by the possibilities," wrote Gil Vega in a Veeam blog post about the strategy's release. "We encourage every organization — government agency, critical infrastructure operator, or private enterprise — to see the release of the strategy as an opportunity: to assess vulnerabilities, invest in recovery capabilities, and foster a culture where resilience is a shared goal."

Learn more

about how Veeam is supporting data resilience across government.