BY ERIC GELLER
SECURITY
MAR 13, 2025 5:30 AM

‘People Are Scared’: Inside CISA as It Reels From Trump’s Purge

Employees at the Cybersecurity and Infrastructure Security Agency tell WIRED they’re struggling to protect the US while the administration dismisses their colleagues and poisons their partnerships.

PHOTO-ILLUSTRATION: WIRED STAFF; GETTY IMAGES

Mass layoffs and weak leadership are taking a severe toll on the US government’s cyber defense agency, undermining its ability to protect America from foreign adversaries bent on crippling infrastructure and ransomware gangs that are bleeding small businesses dry.

Inside the Cybersecurity and Infrastructure Security Agency, vital support staff are gone, international partnerships have been strained, and workers are afraid to discuss threats to democracy that they’re now

prohibited from countering. Employees are even more overworked than usual, and new assignments from the administration are interfering with important tasks. Meanwhile, CISA's temporary leader is doing everything she can to appease President Donald Trump, infuriating employees who say she's out of touch and refusing to protect them.

"You've got a lot of people who … are looking over their shoulder as opposed to looking at the enemy right now," says one CISA employee.

Your Tesla Is Watching

As the Trump administration's war on the federal bureaucracy throws key agencies into chaos, CISA's turmoil could have underappreciated consequences for national security and economic prospects. The agency, part of the Department of Homeland Security, has steadily built a reputation as a nonpartisan source of funding, guidance, and even direct defensive support for cities, businesses, and nonprofits reeling from cyberattacks. That mission is now under threat, according to interviews with seven CISA employees and another person familiar with the matter, all of whom requested anonymity to avoid reprisals.

"Our enemies are not slowing their continuous assaults on our systems," says Suzanne Spaulding, who led CISA's predecessor during the Obama administration. "We need all hands on deck and focused, not traumatized and distracted."

Talent Exodus

CISA's mission has grown significantly since its creation in 2018. Established mainly to defend government networks, the agency increasingly embraced new roles supporting private companies and state governments, advocating for secure software, and cooperating with foreign partners. This helped CISA raise its profile and gain credibility. But now, following several rounds of layoffs and new restrictions from the Trump administration, the agency is struggling to sustain its momentum.

The extent of the cuts at CISA is still unclear—employees are only learning about the loss of colleagues through word of mouth—but multiple employees estimate that, between the layoffs and the Office of Personnel Management's deferred-resignation program, CISA has lost between 300 and 400 staffers—

roughly 10 percent of its 3,200-person workforce. Many of those people were hired through DHS's Cybersecurity Talent Management System (CTMS), a program designed to recruit experts by competing with private-sector salaries. As a result, they were classified as probationary employees for three years, making them vulnerable to layoffs. These layoffs at CISA also hit longtime government workers who had become probationary by transferring into CTMS roles.

Key employees who have left include Kelly Shaw, who oversaw one of CISA's marquee programs, a voluntary threat-detection service for critical infrastructure operators; David Carroll, who led the Mission Engineering Division, the agency's technological backbone; and Carroll's technical director, Duncan McCaskill. "We've had a very large brain drain," an employee says.

> The departures have strained a workforce that was already stretched thin. "We were running into [a] critical skills shortage previously," says a second employee. "Most people are and have been doing the work of two or more full-time [staffers]."

The CISA team that helps critical infrastructure operators respond to hacks has been understaffed for years. The agency added support positions for that team after a Government Accountability Office audit, but "most of those people got terminated," a third employee says.

CISA's flagship programs have been mostly unscathed so far. That includes the threat-hunting branch, which analyzes threats, searches government networks for intruders, and responds to breaches. But some of the laid-off staffers provided crucial "backend" support for threat hunters and other analysts. "There's enhancements that could be made to the tools that they're using," the first employee says. But with fewer people developing those improvements, "we're going to start having antiquated systems."

In a statement, DHS spokesperson Tricia McLaughlin says CISA remains "committed to the safety and security of the nation's critical infrastructure" and touted "the critical skills that CISA experts bring to the fight every day."

National Security Council spokesperson James Hewitt says the reporting in this story is "nonsense," adding that "there have been no widespread layoffs at CISA and its mission remains fully intact."

"We continue to strengthen cybersecurity partnerships, advance AI and open-source security, and protect election integrity," Hewitt says. "Under President Trump's leadership, our administration will make significant strides in enhancing national cybersecurity."

Partnership Problems

CISA's external partnerships—the cornerstone of its effort to understand and counter evolving threats—have been especially hard-hit.

International travel has been frozen, two employees say, with trips—and even online communications with foreign partners—requiring high-level approvals. That has hampered CISA's collaboration with other cyber agencies, including those of "Five Eyes" allies Canada, Australia, New Zealand, and the UK, staffers say.

CISA employees can't even communicate with people at other federal agencies the way they used to. Previously routine conversations between CISA staffers and high-level officials elsewhere now need special permissions, slowing down important work. "I can't reach out to a CISO about an emergency situation without approval," a fourth employee says.

Meanwhile, companies have expressed fears about sharing information with CISA and even using the agency's free attack-monitoring services due to DOGE's ransacking of agency computers, according to two employees. "There is advanced concern about all of our services that collect sensitive data," the third employee says. "Partners [are] asking questions about what DOGE can get access to and expressing concern that their sensitive information is in their hands."

"The wrecking of preestablished relationships will be something that will have long-lasting effects," the fourth employee says.

CISA's Joint Cyber Defense Collaborative, a high-profile hub of government-industry cooperation, is also struggling. The JCDC currently works with more than 300 private companies to exchange threat information, draft defensive playbooks, discuss geopolitical challenges, and publish advisories. The unit wants to add hundreds more partners, but it has "had difficulty scaling this," the first employee says, and recent layoffs have only made things worse. Contractors might be able to help, but the JCDC's "vendor support contracts run out in less than a year," the employee says, and as processes across the government have been frozen or paused in recent weeks, CISA doesn't know if it can pursue new agreements. The JCDC doesn't have enough federal workers to pick up the slack, the fourth CISA employee says.

With fewer staffers to manage its relationships, the JCDC confronts a perilous question: How should it focus its resources without jeopardizing important visibility into the threat landscape? Emphasizing ties with major companies might be more economical, but that would risk overlooking mid-sized firms whose technology is quietly essential to vital US industries.

“CISA continuously evaluates how it works with partners,” McLaughlin says, “and has taken decisive action to maximize impact while being good stewards of taxpayer dollars and aligning with Administration priorities and our authorities.”

Gutting Security Advocacy

Other parts of CISA’s mission have also begun to atrophy.

During the Biden administration, CISA vowed to help the tech industry understand and mitigate the risks of open-source software, which is often poorly maintained and has repeatedly been exploited by hackers. But since Trump took office, CISA has lost the three technical luminaries who oversaw that work: Jack Cable, Aeva Black, and Tim Pepper. Open-source security remains a major challenge, but CISA’s efforts to address that challenge are now rudderless.

The new administration has also frozen CISA’s work on artificial intelligence. The agency had been researching ways to use AI for vulnerability detection and networking monitoring, as well as partnering

with the private sector to study AI risks. “About 50 percent of [CISA’s] AI expert headcount has been let go,” says a person familiar with the matter, which is “severely limiting” CISA’s ability to help the US Artificial Intelligence Safety Institute test AI models before deployment.

The administration also pushed out CISA’s chief AI officer, Lisa Einstein, and closed down her office, the person familiar with the matter says. Einstein’s team oversaw CISA’s use of AI and worked with private companies and foreign governments on AI security.

A large team of DHS and CISA AI staffers was set to accompany Vice President JD Vance to Paris in February for an AI summit, but those experts “were all pulled back” from attending, according to a person familiar with the matter.

‘Nefarious’ Retribution

CISA staffers are still reeling from the agency’s suspension of its election security program and the layoffs of most people who worked on that mission. The election security initiative, through which CISA provided free services and guidance to state and local officials and worked with tech companies to track online misinformation, became a target of right-wing conspiracy theories in 2020, which marked it for death after Trump’s return to the White House.

The program—on hold pending CISA’s review of a recently completed internal assessment—was a tiny part of CISA’s budget and operations, but the campaign against it has alarmed agency employees. “This is definitely in the freak-out zone,” says the first employee, who adds that CISA staffers across the political spectrum support the agency’s efforts to track online misinformation campaigns. “All of us recognize that this is a common deception tactic of the enemy.”

The election security purge rippled across the agency, because some of the laid-off staffers had moved from elections to other assignments or were simultaneously working on both missions. Geoff Hale, who led the elections team between 2018 and 2024, was serving as the chief of partnerships at the JCDC when he was placed on administrative leave, setting off a scramble to replace him.

The removal of Hale and his colleagues “was the start to a decline in morale” at CISA, according to the second employee. Now, staffers are afraid to discuss certain topics in public forums: “No one's going to talk about election security right now,” the first employee says.

“The fact that there’s retribution from the president … is kind of frightening,” this employee adds. “A very nefarious place to be.”

Abandoned and Demoralized

The layoffs, operational changes, and other disruptions at CISA have severely depleted morale and undermined the agency’s effectiveness. “Even simple tasks feel hard to accomplish because you don't know if your teammates won't be here tomorrow,” says the fourth employee.

The biggest source of stress and frustration is acting CISA director Bridget Bean, a former Trump appointee who, employees say, appears eager to please the president even if it means not defending her agency. Bean “just takes whatever comes down and implements [it] without thought of how it will affect [CISA’s] mission,” the fifth employee says. Employees describe her as a poor leader and ineffective communicator who has zealously enacted Trump’s agenda. In town-hall meetings with employees, Bean has said CISA must carefully review its its authorities and urged staffers to “assume noble intent” when dealing with Trump officials. While discussing Elon Musk’s mass-buyout program, she allegedly said, “I like to say ‘Fork in the Road’ because it's kind of fun,.” according to the fourth employee. She was so eager to comply with Musk’s “What did you do last week?” email that she instructed staffers to respond to it before DHS had finalized its department-wide approach. DHS later told staff not to respond, and Bean had to walk back her directive.

“Bean feels like she's against the workforce just to please the current administration,” the second employee says. The fourth employee describes her as “not authentic, tone-deaf, spineless, [and] devoid of leadership.”

McLaughlin, the DHS spokesperson, says CISA “is not interested in ad hominem attacks against its leadership,” which she says “has doubled down on openness and transparency with the workforce.”

The return-to-office mandate has also caused problems. With all employees on-site, there isn’t enough room in CISA’s offices for the contractors who support the agency’s staff. That has made it “very difficult” to collaborate on projects and hold technical discussions, according to the first employee. “There wasn’t much thought about [RTO’s] impact to operations,” says the fourth employee. According to a fifth employee, “executing some of our sensitive operations is now harder.” (“CISA has worked tirelessly to make the return to office as smooth as possible from space to technology,” McLaughlin says.)

Employees are dealing with other stressors, too. They have no idea who's reading their Musk-mandated performance reports, how they're being evaluated, or whether AI is analyzing them for future layoffs. And there's a lot of new paperwork. "The amount of extra shit we have to do to comply with the 'efficiency measures' … [takes] a lot of time away from doing our job," says the fifth employee.

Bracing for More

When Trump signed the bill creating CISA in November 2018, he said the agency's workforce would be "on the front lines of our cyber defense" and "make us, I think, much more effective." Six and a half years later, many CISA employees see Trump as the biggest thing holding them back.

"This administration has declared psychological warfare on this workforce," the fourth employee says.

With CISA drawing up plans for even larger cuts, staffers know the chaos is far from over.

"A lot of people are scared," says the first employee. "We're waiting for that other shoe to drop. We don't know what's coming."

Entire wings of CISA—like National Risk Management Center and the Stakeholder Engagement Division—could be on the chopping block. Even in offices that survive, some of the government's most talented cyber experts—people who chose public service over huge sums of money and craved the lifestyle of CISA's now-eliminated remote-work environment—are starting to see their employment calculus differently. Some of them will likely leave for stabler jobs, further jeopardizing CISA's mission. "What is the organization going to be capable of doing in the future?" the first employee asks.

If Trump's confrontational foreign-policy strategy escalates tensions with Russia, China, Iran, or North Korea, it's likely those nations could step up their use of cyberattacks to exact revenge. In that environment, warns Nitin Natarajan, CISA's deputy director during the Biden administration, weakening the agency could prove very dangerous.

"Cuts to CISA's cyber mission," Natarajan says, "will only negatively impact our ability to not only protect federal government networks, but those around the nation that Americans depend on every day."