Federal shutdown deals blow to already hobbled cybersecurity agency

Richard Forno, Teaching Professor of Computer Science and Electrical Engineering, and Associate Director, UMBC Cybersecurity Institute, University of Maryland, Baltimore County

The federal cybersecurity agency is crippled by layoffs and shutdown furloughs.

The Conversation, CC BY-ND

As the United States experiences its latest government shutdown, most of the daily operations of the federal government have ground to a halt. This includes much of the day-to-day work done by federal information technology and cybersecurity employees, including those at the nation's leading civilian cybersecurity agency, the Cybersecurity and Infrastructure Security Agency.

CISA is among the entities that will see the deepest staffing reductions during the shutdown that began Oct. 1, 2025, according to Department of Homeland Security documentation. Only about one-third of its employees remain on the job after federal employees were furloughed. As if cybersecurity wasn't challenging enough, fewer CISA employees are being asked to do more and more work protecting American cyberspace during the shutdown. And they'll be working with the promise of getting paid for their efforts at some date in the future once the shutdown ends.

The current CISA situation is grim, from my vantage point as a cybersecurity researcher and former industry practitioner. The agency was already experiencing deep cuts to its staff and resources before the shutdown. And now, coinciding with the shutdown, a key law that enabled the agency to facilitate information-sharing with the private sector has expired.

Taken together, the cyberdefense agency is being hobbled at a time when the need for its services has never been greater, from the ongoing China-led Salt Typhoon attack on U.S. telecommunications networks to ransomware, data breaches and threats to infrastructure.

CISA was created in 2007 within the Department of Homeland Security. As its name implies, the agency is charged with digital security matters across the federal government. The agency also works with the companies that operate and secure the numerous critical infrastructure sectors of the American economy, such as phone networks, the electric grid and energy pipelines. Additionally, it helps state and local governments across the country secure their vulnerable networks and data.

CISA also publishes threat and vulnerability alerts for the government and cybersecurity community and engages with public and private stakeholders on best practices in response to emerging vulnerabilities. Prior to the recent expiration of the 2015 Cybersecurity Information Sharing Act, the agency also made it easier for organizations to share useful information with the government to help cybersecurity teams better protect their systems.

Political football

The agency takes a nonpartisan approach to cybersecurity matters. However, some politicians have accused the agency of political bias for its work helping states protect their voting infrastructure from cyberattacks and external influence. Specifically, the agency was repeatedly maligned for calling the 2020 election the "most secure" in history. For some in elected office, this work on election security has tarnished CISA's reputation and perhaps explains recent budgetary actions taken against the agency.

Since the Trump administration took office in January 2025, nearly 1,000 CISA employees have departed the agency through voluntary buyouts or deferred resignations. By the end of May 2025, nearly all of CISA's senior leadership had resigned or had announced plans to do so.

For 2026, the president's draft budget proposes to reduce CISA's head count by nearly one-third, dramatically cutting staff from its risk management and stakeholder engagement divisions. Other cuts will significantly reduce the agency's collaboration activities and funding for CISA's various cybersecurity education and training programs.

Making the problem worse, the government shutdown began at the same time that Congress failed to renew the Cybersecurity Information Sharing Act. This law provided a legal shield that allowed companies and infrastructure operators to share timely and often sensitive information with CISA about the cyberattacks, vulnerabilities and incidents that they were encountering.

In the wake of the law's expiration, prudent companies may consider restricting what information they share with the government. Without the indemnification provided by CISA, many companies will likely have their legal teams review any information to be shared with the government. And that takes time.

Unfortunately, adversaries do not reduce their attacks against the U.S. based on available federal cyber defense funding or the status of cybersecurity laws. In fact, malicious hackers often strike when their target's guard is down.

Charting a better course

Early in my career I had to work through a prolonged government shutdown. I've also participated in and developed assorted public-private information-sharing environments to exchange intelligence and analysis on cyber- and national security matters. And having been in the D.C. area for over 30 years, I've seen how government works. So I have a good idea of what's needed to improve American cybersecurity. The following suggestions are a starting point.

First, Congress could ensure that critical security agencies such as CISA are immune from the threat of recurring federal government shutdowns. If it desired, Congress could set budgets for America's security agencies on a biennial basis – as 16 states already do for their entire budgets.

In terms of cybersecurity funding, the White House's proposed 2026 budget reduces research and education on cybersecurity. For example, the nation's premiere federal cybersecurity scholarship program to recruit, educate and place future federal cybersecurity workers would be reduced by over 60%. Protecting this funding would allow CISA and the federal government to maintain the pipeline for a robust and capable cybersecurity workforce both today and into the future.

Companies could develop new or expand existing nongovernmental information-sharing networks that are not completely dependent on the government to facilitate or fund, such as the Cyber Threat Alliance or the Center for Internet Security. Cybersecurity relies on trust. But right now, the instability of the federal government makes it difficult to rely on any entity under its policy or funding influence, no matter how well time-tested and trusted. Regardless, without legal protections, the information-sharing utility of these services will be limited.

Cybersecurity risks remain even if the federal government shuts down. So this is another reminder that each of us is responsible for our own cybersecurity. Individual users should continue to remain vigilant, follow accepted best practices for cybersecurity and always be mindful about online risks.

It's ironic that the federal government is shutting down, CISA is being eviscerated and the Cybersecurity Information Sharing Act has expired just as the country begins to observe national Cybersecurity Awareness Month – another collaborative public engagement activity that CISA promotes to help improve cybersecurity for all Americans.

Richard Forno has received funding related to cybersecurity research and education from the National Science Foundation (NSF), the Department of Defense (DOD), the US Army, State of Maryland, and private companies during his academic career since 2010. From 2012-2025 he co-directed UMBC's Scholarship For Service program.