Reinvigorating Federal Cybersecurity Initiatives: *A Post-Shutdown Call To Action for the Trump Administration and Congress*

After the government shutdown, new leadership is needed to protect our nation from increasing cyber threats. According to the House Committee on Homeland Security's *2025 Cyber Threat Snapshot*, malicious cyber activity linked to the People's Republic of China increased by 150% between 2023 and 2024, and so far in 2025, significant cyberattacks have targeted state and local governments in at least 44 U.S. states.[1] Nation-state actors and cybercriminal groups are also rapidly developing new Tactics, Techniques, and Procedures (TTPs), which increasingly leverage AI, to infiltrate government systems, disrupt critical infrastructure, and exploit private enterprises and citizens alike.

As federal operations resume, it is imperative that the federal government renew its commitment to cybersecurity and operational resilience, dedicating the necessary attention and resources to protect Americans and safeguard U.S. economic and national security against these growing threats. To that end, the Cybersecurity Coalition outlines four key areas of action for the Trump Administration and Congress to strengthen the nation's cybersecurity posture in the coming months:

1. Equip Federal Agencies to Fulfill Cybersecurity Missions

Every federal agency bears some responsibility for cybersecurity, beginning with securing its own systems and data. This includes consistently mitigating known exploited vulnerabilities on federal information systems. Several agencies also have mandates to support and coordinate cybersecurity efforts across the federal enterprise or share responsibility for strengthening the cybersecurity of the private sector in their capacity as Sector Risk Management Agencies (SRMAs). To fulfill these numerous and varied missions, federal agencies rely on substantial technical and human resources as well as clear overarching guidance. The shutdown, however, has disrupted the federal government's efforts to procure cybersecurity capabilities, secure newly created cloud services, hire personnel to fill mission-critical vacancies, and publish new guidance documents.

Procurement - The shutdown has delayed the approval and renewal of numerous contracts for critical cybersecurity products and services, impeding agencies' ability to modernize and sustain their defenses. Therefore, the Cybersecurity Coalition recommends that the Trump

[1] House Committee on Homeland Security, *Cyber Threat Snapshot, Malign Nation-States and Opportunistic Criminal Networks: A Persistent Cyber Threat in America,* October 31, 2025, https://homeland.house.gov/wp-content/uploads/2025/10/Cyber-Threat-Snapshot.pdf

Administration move swiftly to resume and expedite delayed cybersecurity procurements and ensure that ongoing contract processes continue without interruption.

Staffing - The shutdown has also slowed hiring efforts for key cybersecurity positions across the federal government. While cybersecurity positions at agencies were exempt from reductions in force, many positions were vacated by the retirements and departures of experienced personnel. To address the gap, the Cybersecurity Coalition urges the Administration to take immediate steps to fill critical vacancies, strengthen retention of cybersecurity professionals, and reinstate exemptions that protect cybersecurity personnel from layoffs.

Post Quantum Cryptography (PQC) - The shutdown has further delayed the White House Office of Management and Budget's (OMB) development of guidance pursuant to the Quantum Computing Cybersecurity Preparedness Act, which would require each agency to prioritize technology for migration to PQC and develop a plan for its transition based on that prioritization. The Cybersecurity Coalition recommends that the Administration prioritize completing this guidance and provide agencies with additional resources to support their transition to PQC.

2. Bolster Legislative Action on Cybersecurity

Legislative action has been instrumental in advancing cybersecurity policy in the United States over the past decade. Congress has provided liability protections for companies that share threat information, directed resources to help state and local governments build cybersecurity capacity, and taken steps to modernize the federal government's overall approach to cyber risk management. However, the shutdown has diverted legislators' attention away from cybersecurity, delaying efforts to renew essential programs and to develop new legislative frameworks capable of addressing emerging challenges.

Cybersecurity Information Sharing Act of 2015 - Authorities under the Cybersecurity Information Sharing Act of 2015 that enabled the exchange of cyber threat indicators and defensive measures between the private sector and federal government expired at the end of September. The Continuing Resolution extends coverage into January, but more certainty is needed to promote sharing among companies and with the government. The Cybersecurity Coalition urges Congress to act expeditiously to reauthorize the Act's authorities for another ten years through a clean renewal, ensuring continuity in public-private information sharing.

State and Local Cybersecurity Grant Program (SLCGP) - The SLCGP also expired and was temporarily extended in the Continuing Resolution. State, local, territorial, and tribal (SLTT) governments, most of which are under-resourced and lack sufficient cybersecurity capacity, have become increasingly vulnerable to sophisticated cyberattacks and rely on SLCGP grants for protection. Accordingly, the Cybersecurity Coalition urges Congress to fully renew the program for another ten years and provide meaningful appropriations to ensure it remains effective.

Oversight and New Areas for Legislation - The cyber threat landscape continues to evolve rapidly, driven by new technologies such as AI and quantum computing and by increasingly sophisticated adversaries, including those backed by the People's Republic of China, the Russian Federation, the Islamic Republic of Iran, and the Democratic People's Republic of Korea. Congress also bears responsibility for ensuring that the executive branch remains accountable for achieving its cybersecurity objectives. The Cybersecurity Coalition encourages lawmakers to renew oversight of the Cybersecurity and Infrastructure Security Agency's (CISA) rulemaking process for the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) and to monitor the performance of the Office of the National Cyber Director (ONCD) to ensure it is fulfilling its statutory mandate.

3. Clarify Cybersecurity Leadership Roles and Ensure Strategic Cohesion

Cybersecurity initiatives can only succeed when experienced leadership guides their development and implementation pursuant to a coherent strategic vision. In recent years, however, federal agencies have pursued divergent priorities, resulting in fragmented efforts and diluted focus. As the government resumes full operations following the shutdown, the Administration has a key opportunity to restore leadership and ensure that all agencies are aligned toward shared national cybersecurity objectives.

Leadership Vacancies - Key cybersecurity leadership positions remain unfilled across the federal government, including at CISA, U.S. Cyber Command (CYBERCOM), and the National Security Agency (NSA). This hinders their ability to advance initiatives, coordinate with other agencies, and ultimately respond to emerging threats. Therefore, the Cybersecurity Coalition urges the Trump Administration and Congress to work together to swiftly fill these critical posts, ensuring operational continuity and strengthening national cyber readiness.

Centralization Under ONCD - In remarks at the 2025 Meridian Summit, National Cyber Director Sean Cairncross emphasized the need to elevate ONCD "to the place it was envisioned by Congress and the Executive when it was created." Notably, this involves empowering ONCD to serve as the federal government's central authority for cybersecurity policy and coordination. The Cybersecurity Coalition supports this approach and urges the Trump Administration to ensure that all agencies align behind ONCD's leadership, especially the positions reflected in the forthcoming revision of the *National Cybersecurity Strategy.*

Cybersecurity Actions from AI Action Plan - The White House's AI Action Plan calls for bolstering critical infrastructure cybersecurity through the use of AI defensive tools to stay ahead of emerging threats. The Cybersecurity Coalition urges the Administration to prioritize advancing policy actions to support the adoption of these tools to maintain robust defenses, especially for owners and operators of critical infrastructure with limited financial resources.

Regulatory Alignment - Divergent cybersecurity requirements across federal regulators make it difficult for organizations to implement consistent security measures and often lead to delays as they navigate overlapping compliance regimes. This fragmented approach also exacerbates the ongoing cybersecurity talent shortage by reallocating personnel from core security to administrative functions. A more unified and efficient approach, particularly for cyber incident reporting (e.g., aligning definitions, standardizing reporting thresholds for reporting, and setting consistent timelines), would alleviate this pressure. Accordingly, the Cybersecurity Coalition urges the Administration to prioritize streamlining federal cyber regulations and compliance burdens.

4. Revitalize Engagements with the Private Sector

The United States has long been a global cybersecurity leader in large part because of consistent and structured collaboration between the federal government and the private sector. However, the recent government shutdown disrupted many planned dialogues and engagements. As government operations resume, the Administration should prioritize rebuilding and strengthening these channels of engagement to maintain the nation's cybersecurity leadership.

Critical Infrastructure Partnership Advisory Council (CIPAC) - CIPAC has historically played a vital role in facilitating cooperation between the government and critical infrastructure owners and operators, helping to mitigate vulnerabilities, and promoting essential communication during emergencies. While the Trump Administration is in the process of overhauling CIPAC's structure, the current absence of a replacement framework has disrupted this essential collaboration. The Cybersecurity Coalition urges the Administration to finalize and implement a new structure to resume this invaluable collaboration.

CIRCIA Rulemaking - CISA is now set to finalize regulations to implement certain aspects of CIRCIA by May 2026. Active engagement with industry stakeholders is essential to ensure that these regulations are practical and effective. The Cybersecurity Coalition urges the Administration to ensure that robust and ongoing *ex parte* discussions and another open comment period occur prior to finalization of the rules.

Conclusion

The reopening of the federal government presents an opportunity to realign and reenergize the nation's cybersecurity agenda. By focusing on the four key areas outlined in this paper the Trump Administration and Congress can restore momentum and strengthen the nation's overall cyber resilience. This will not only safeguard federal systems and critical infrastructure but also ensure that the United States remains a global leader in cybersecurity for years to come.