Jiwon Ma & RADM (Ret.) Mark Montgomery

Top 5 Recommendations for the Trump Administration and Congress

Over the past five years, the Cyberspace Solarium Commission helped lay the foundation for stronger U.S. cyber policy, spurring real progress across government and industry. Yet weak statutory authorities, diminished diplomatic capacity, and growing workforce and regulatory gaps continue to threaten national resilience. Addressing these challenges will require action from both Congress and the administration. The following five priorities mark the next phase in strengthening America's cyber defense in the years ahead.

1. Enhance the Authorities of the Office of the National Cyber Director

The ONCD, created in the fiscal year (FY) 2021 National Defense Authorization Act (NDAA), has grown into a permanent fixture of U.S. cyber governance. Although the office has proven effective at convening agencies and shaping strategy, it still lacks the positional authority and interagency relationships needed to enforce decisions across the government. This gap undermines efficiency and slows progress on urgent tasks. The same is true for resources: ONCD can review agency budget submissions but has no authority to align cyber investments across departments, leaving federal resources missing, fragmented, or duplicative. Regulatory oversight presents similar challenges. Without a mandate to harmonize regulations, ONCD cannot resolve the patchwork of conflicting requirements facing critical infrastructure operators, a problem that industry has repeatedly warned is eroding trust in government guidance. To address these shortcomings, the ONCD should lead efforts to rewrite the decade-old policy document, known as Presidential Policy Directive 41, to clarify responsibilities for the national incident response process. President Donald Trump should issue an executive order to grant ONCD formal convening authority over civilian agency cyber policy, review authority over agency cyber budgets, and a mandate to lead regulatory harmonization efforts through an interagency working group. Elevating ONCD's role with these actions would provide the clarity and authority needed for ONCD to fulfill its role as the central driver of national cyber policy.

2. Restore the Workforce and Funding of the Cybersecurity and Infrastructure Security Agency

CISA is the federal government's cyber defense agency, responsible for leading national incident response, issuing threat advisories, and developing resilience programs across sectors. National Security Memorandum 22 reaffirmed this role, designating CISA as the national coordinator for the security and resilience of critical infrastructure. Yet CISA's effectiveness has been weakened by steep workforce and budget cuts that undermine its ability to support operators on the ground. These pressures limit CISA's ability to scale critical programs that give the administration early visibility into attacks and to share information with private sector partners. By investing in CISA in its role as national coordinator, the administration can prevent disruptions, protect American families, and ensure economic stability. The administration should develop a plan of action and restore staffing and budget levels, with the goal of establishing and reinforcing CISA's role as national coordinator for the security and resilience of critical infrastructure. Congress should provide multi-year funding stability to prevent further erosion of capacity. Empowering CISA strengthens the administration's hand in deterring adversaries and demonstrates visible leadership in keeping the country safe.

3. Restore Funding and Personnel Dedicated to Cyber Diplomacy and Capacity Building at the State Department

Congress codified the State Department's CDP with the Cyber Diplomacy Act of 2022. CDP's mission is to strengthen capacity and confidence among allies and partners. Since its codification, CDP has developed key

strategies and led engagements with partners — from standing up incident response capabilities to jointly countering authoritarian narratives online. CDP leveraged a dedicated cyber-assistance fund to help nations rapidly mitigate attacks and paired U.S. seed funding with allied and private-sector investment to crowd out Chinese firms seeking to dominate telecommunications and emerging technology supply chains. However, CDP's effectiveness has been constrained by a restructuring effort that fractured cyber expertise across the State Department and stripped away resources that would allow the bureau to coordinate policy and programs effectively, reducing available partner cyber capacity funds. Meanwhile, adversaries like China continue to expand their global digital influence and dominate international technical standard-setting bodies, filling the vacuum left by U.S. retrenchment. The administration should restore CDP's personnel and resources through reprogramming, supplemental requests, or executive orders, while Congress complements this effort by creating a long-term funding line that ensures the continuity of cyber-capacity building programs. To rebuild trust, the Trump administration must demonstrate to allies that Washington is a reliable partner in building secure digital infrastructure that supports U.S. trade and investment.

4. Maintain and Restore Critical Support to Public Collaboration Effort

The Critical Infrastructure Partnership Advisory Council (CIPAC) has provided a legal framework for information exchange between the federal government and private-sector partners for nearly two decades. The Trump administration's decision to eliminate CIPAC created legal uncertainty around information sharing, undermining long-standing trust between industry and government. Since its elimination, critical infrastructure operators have scaled back their engagement with the federal government out of concern that sensitive company data could be publicly exposed. f the Department of Homeland Security fails to immediately reinstate CIPAC, Congress should intervene to restore clear legal protections for industry-government dialogue. Congress should also pass a long-term reauthorization of existing cybersecurity information sharing protections.

5. Expand the Talent Pool and Improve Retention of the Cyber Workforce

Since the start of the Trump administration, several workforce decisions have reshaped how the federal government recruits and retains cyber talent. New hiring practices and at-will mandates shift emphasis away from technical qualifications and discourage qualified candidates from pursuing career roles. The rollback of diversity, equity, and inclusion initiatives eliminated programs that had broadened the pipeline of skilled candidates from underrepresented and non-traditional backgrounds, narrowing access to key talent pools. The result is a growing gap in filling critical cyber positions from an already limited talent pool. While the administration has wisely called for both "skills-based" and "merit-based" hiring, it has yet to establish a consistent workforce model to deliver on those goals — risking what had been a rare area of bipartisan consensus around building a skills-based cyber workforce. Clarifying a consistent, skills-based model — and broadening the pipelines for non-traditional candidates through apprenticeships, training, and scholarship-for-service programs — will be essential to stabilizing the cyber workforce and ensuring agencies have the expertise to defend the nation's most critical systems. Also, the government should expand proven skills-based recruitment programs like CyberCorps.