



CYBER GOVERNANCE

ISSUES FOR THE TRUMP ADMINISTRATION

John K. Costello

MARCH • 2025

ABOUT THE AUTHOR



JOHN COSTELLO is a Senior Advisor to Solarium 2.0, Adjunct Senior Fellow at the Center for a New American Security, and a Principal at WestExec Advisors. Mr. Costello previously served as the first chief of staff and principal architect of the Office of the National Cyber Director (ONCD), the first White House

component created since 1988. Prior to his time at ONCD, Mr. Costello served as the deputy executive director of the Cyberspace Solarium Commission, where he led the commission's work on cybersecurity, resilience, and supply chain security, as well as the commission's legislative efforts. Mr. Costello served as the deputy assistant secretary of intelligence and security at the Department of Commerce. In that capacity, Mr. Costello established the Commerce Department's intelligence analysis capability and led the department's information and communications technology and service supply chain analytical and regulatory efforts. Mr. Costello is a U.S. Navy veteran, serving his tours of duty at the National Security Agency as an intelligence analyst and operations officer. While at the National Security Agency, he specialized in foreign adversary cyber, electronic, and information warfare. John has a working professional proficiency in Mandarin Chinese and graduated with honors from the Defense Language Institute.

OBJECTIVES & METHODOLOGY

The purpose of this report is to examine the current state of U.S. cyber governance, identify key issues, and provide practical and politically viable recommendations for the Trump Administration and the 119th Congress. This report is informed by desk research on existing law and policy, unpublished studies and findings of the Cyberspace Solarium Commission, and interviews with current and former government officials, public policy experts, industry experts, and academics. The author welcomes any questions and comments on the report.

ACKNOWLEDGEMENTS

The author is grateful to Mark Montgomery, Samantha Ravich, Annie Fixler, Michael Abonyi and the the team at the Foundation for Defense of Democracies Center on Cyber and Technology Innovation for their support in the production of this report. The author extends sincere thanks to Trey Herr, Chris Inglis, Rob Knake, Harry Krejsa, Nick Leiserson, Jim Lewis, Joe McReynolds, Brandon Pugh, and Kevin Reifsteck for taking the time to read and/or provide input on this report. Thanks also to Tatyana Bolton, Mike Flynn, Chris Roberti, Rob Sheldon, Jordana Siegel, Charley Snyder, and Rob Strayer for their input and perspective during the research stage of the report. This report was produced with funding provided by Microsoft. The views, content, conclusions, and recommendations contained herein are the sole responsibility of the author.

CONTACT

For comments, inquiries, or questions pertaining to this report, please contact the author at jkcostie@gmail.com.



MARCH · 2025

THE STATE OF CYBER GOVERNANCE

Cyber governance remains a persistent challenge for every administration. As cyber threats evolve, agency missions mature, and technology advances, governance models must be responsive in adapting while ensuring long-term sustainability and coordination. Cybersecurity's unique positioning as a multi-agency, cross-sectoral issue further complicates governance, as agencies may hold conflicting equities—whether through their enterprise cybersecurity responsibilities, primary cyber missions (CISA, NSA, CYBERCOM), adjacent functions (FDA, DOE), or occasional involvement in cyber-related national security efforts (OFAC sanctions, law enforcement investigations). This ever-changing threat landscape, quickly evolving technology ecosystem, lack of centralized planning and role assignments, and the resulting dispersion of responsibility has led to duplicative efforts, regulatory inconsistencies, and inefficiencies in both policy and operations.

Despite numerous legislative and executive measures aimed at improving interagency alignment, efforts to centralize authorities and streamline coordination have often exacerbated fragmentation—adding additional coordinating bodies rather than consolidating existing functions. This challenge is rooted in both the executive branch, where agencies resist ceding authority, and in Congress, where jurisdictional divisions favor narrow, incremental legislative changes over broader restructuring efforts. It is further exacerbated by the Constitutional bias for firewalls between private and public sector activities (e.g., the private sector is expected to pursue its aims with minimal disruption from the public sector and no expectation of continuous collaboration in framing and executing sector initiatives). Discord in governance is a result of a steady expansion of authorities and budgets without a corresponding improvement in strategic unity or operational efficiency. Cyber governance in the United States has thus evolved not from a central plan but through an incremental, additive process—layering new authorities, structures, and initiatives atop existing ones rather than undertaking comprehensive reform. This approach while adaptive often lacks coherence and efficiency.

“Discord in governance is a result of a steady expansion of authorities and budgets without a corresponding improvement in strategic unity or operational efficiency.”

“The U.S. must leverage creative governance solutions that maximize coordination without triggering the bureaucratic resistance that has historically stymied reform.”

Attempts to establish a stronger central coordinating function frequently face resistance from agencies and their legislative allies, who seek to defend autonomy, authority, and funding. Efforts to create more robust governance structures encounter dual opposition: from executive branch entities wary of losing influence and from Congressional stakeholders reluctant to reopen statutes that could expose broader agency authorities to revision. This opposition is especially pronounced when proposals risk encroaching on traditionally independent functions, such as law enforcement investigations, regulatory autonomy, or Presidential national security prerogatives. Consequently, any attempt to grant overarching authority to a single agency—whether within the White House or elsewhere—is unlikely to succeed and risks being diluted into incremental, limited improvements rather than transformative change.

Given the first Trump Administration's unconventional approach to governance and creative statutory interpretation, the second term has a unique opportunity to drive meaningful improvements in how the federal government secures and defends cyberspace. Given the political and structural realities that make sweeping reorganization unlikely, both the Trump Administration and Congress must find ways to enhance cohesion, alignment, and operational effectiveness within existing authorities. The U.S. must leverage creative governance solutions that maximize coordination without triggering the bureaucratic resistance that has historically stymied reform. In this context, the path forward lies in pragmatic, targeted initiatives that work within existing structures to drive greater cohesion and efficiency. This includes binding (or aligning) the authority of the Office of the National Cyber Director to the administration's strategy and priorities, clarifying and reinforcing the role of the National Cyber Director in the defense and execution of those priorities, establishing a more structured and accountable interagency cyber community, setting clear and actionable national cyber priorities, and advancing regulatory harmonization to reduce fragmentation.

RECOMMENDATION 1

AFFIRM THE NATIONAL CYBER DIRECTOR POSITION IN EXECUTIVE ORDER

The National Cyber Director (NCD) was intended, in part, to streamline, consolidate, and centralize the myriad authorities in the White House into a cohesive center of governance for U.S. government cyber activity.¹ However, in the four years since its creation there continue to be substantial concerns about the position's authority, roles, and responsibility—particularly with respect to other offices in the Executive Office of the President (EOP).² Compounding this issue was revival in 2021 of the National Cyber Coordinator position—in the form of the Deputy National Security Advisor for Cyber and Emerging Technologies—a position the NCD was intended to replace.³ The NCD's authorizing statute, while important in conveying Congressional intent, offers little help in resolving ambiguities. Congress is constitutionally limited in dictating how the President makes use of a position it creates and how such a position is integrated into the President's staff—if at all. This constraint, and the more practical need to overcome jurisdictional and executive objections in the legislative process, explain the absence of detail in defining the NCD's relationships across the EOP.⁴

The NCD, and similar senate-confirmed White House positions on which it was modeled⁵, fall into unique area of constitutional law, one where Congressional authority to make laws and dictate the organization of government intersects with Presidential discretion over their staff and with whom they rely upon for advice.⁶ It is for this reason the President has, within limits, considerable latitude in interpreting and further defining the authorities, roles, and responsibilities of these positions—and has often done so through an “establishing” Executive Order within two to four years after the position was formally codified into law.⁷ Such an imprimatur helps to more concretely define the working relationships between these Senate-confirmed positions and the Title 3 staff positions (NSC, etc.) that fall solely under the President's discretion.

Four years on, the ONCD has yet to benefit from such an order, leaving significant uncertainty regarding its authorities, responsibilities, and integration within the broader executive framework—a fact that threatens its ability to drive a cohesive national cyber strategy and subjects the office to potentially conflicting interpretations of its role and mandate.

The President should issue an Executive Order affirming the role of the National Cyber Director, articulating and further defining the position's authorities and responsibilities. In doing so, the President should, when and where possible, seek to align the White House's conception of the position with key elements of the NCD's authorizing statute, namely advising the President on cybersecurity and defense, budget review and assessment, development and coordination of national cyber strategy, planning and preparation by the U.S. government in the preparation for and response to significant cyber campaigns, and serving as the principal public face for the U.S. government on cybersecurity issues.

Presidential Advisor: The Executive Order should formally affirm the NCD primacy on cyber issues by designating the role as the principal advisor to the President on matters related to cyber defense and security. This should carry with it the expectation of the NCD's participation and involvement in policy issues and actions that substantially deal with those topics.

Updating Executive Process: The Executive Order should identify and update existing presidential actions to formally incorporate the NCD where the position has a clear mandate. These include, but are not limited to, the Cyber Response Group (CRG) outlined in Presidential Policy Directive 41 (PPD-41)⁸, the Vulnerabilities Equities Board⁹, and the Cyber Safety Review Board (CSRBB)¹⁰. Such an approach cements the NCD's role as a central participant in cybersecurity decision-making while maintaining the established flow of executive governance.

Budget Review and Assessment: The Executive Order should solidify the NCD's authority to review, coordinate, and advise on federal cyber budgets, ensuring government-wide resource alignment with national cybersecurity objectives. This form of budgetary oversight would be modeled after that afforded to similar positions, such as the Director of National Intelligence (DNI).

Dual-hat Arrangement: The Executive Order should formally codify the Federal Chief Information Security Officer (CISO) as dual-hatted to the Office of the National Cyber Director (ONCD), marrying the strengths of the ONCD—visibility, personnel, expertise—with the institutional power, processes, and authorities available to the Federal CISO. Such an arrangement proved effective during the last four years of the position, strengthening both roles and preempting potential concerns over turf and encroachment.¹¹

RECOMMENDATION 2

REINFORCE AND FOCUS THE CYBER ROLE OF THE NATIONAL SECURITY COUNCIL

Providing greater clarity for the NCD will undoubtedly strengthen its standing within the White House, but it cannot, on its own, resolve lingering questions about how the role is intended to work with the National Security Council (NSC). The NSC has traditionally held a remarkably expansive role in cyber affairs, one best illustrated by the *breadth* of policy issues it took on—cybersecurity and defense, military offense, intelligence operations, cost imposition outside of cyberspace, etc.—as well as the sheer *depth* of its functional role—policy and strategy development, implementation, oversight of programmatic priorities, and the coordination among departments and agencies for routine incident response, significant events, and operational actions and campaigns. The scope, a natural extension of the NSC's core responsibilities for policy coordination and oversight, has continued to grow in tandem with the frequency, scope, and scale of incidents and the number of departments and agencies with national security equities in cyberspace.

This breadth of responsibility—made necessary by the lack of a central, coordinating body that could take on more routine, programmatic, and operational elements of coordination and oversight—is outdated and inefficient at a time when the ONCD exists. While there is no doubt that the NSC has preeminent authority and oversight over all aspects of national security policy—to include cybersecurity and defense—it is often resource-constrained, over-tasked, and limited in the time and attention it is able to devote to any given issue. In practice, the NSC must focus on the most urgent, high-priority national security concerns, a reality that can conflict with the extensive needs of coordinating the U.S. government's cybersecurity mission and the fact that these efforts rarely rise to the level of an imminent national security crisis. The ONCD was designed and created, in part, to alleviate this pressure and grant the NSC greater latitude to maintain unity of focus and flexibility in response to Presidential priorities and emerging events. To fully empower both organizations and play to their respective strengths, the long-standing operating model of the NSC's cyber role—in place since the early 2010's—must be updated and revised accordingly.

The President should issue an Executive Order clearly defining the roles and responsibilities of the ONCD and NSC, outlining individual and shared responsibilities in terms of both policy issue and functional roles. This model should broadly align with that articulated by former NCD Chris Inglis—where the NSC's focus remains on cyber issues that more centrally implicate U.S. national security policy, such as foreign policy, intelligence, and military operations (issues “outside of cyberspace”), while the ONCD concentrates on cyber defense and security issues (issues “in and through cyberspace”). The ONCD would assume the more routine, operational, and procedural coordination tasks requiring a level of sustained attention and depth that is impractical in regular NSC process.

Complementary Roles: This arrangement creates a complementary rather than competitive relationship: reaffirming and strengthening the NSC's responsibility and in setting national security strategy and policy across all elements of national power, while empowering the ONCD in managing and co-ordinating cybersecurity and defense with a community of departments and agencies within that overarching framework.

Cyber Preparation and Response: The President should designate the NCD as lead for the Cyber Response Group (CRG), the inter-agency body that meets regularly to handle and respond to incidents that fall below “significant” and around which preparatory cyber efforts are organized and overseen. This would enable the NCD to take on the more routine work of coordination across department and agencies, while preserving the NSC's role in handling incidents when they cross the threshold into a certain level of scope or impact—and broader instruments of national power must be brought to bear.

Defense Focused-Offense Aware¹²: The ONCD was designed to help harmonize U.S. policy, operations, and planning between offensive and defensive elements. In articulating the NSC and NCD's role, the President should ensure the NCD is “defense focused-offense aware” —able to account for, shape, and influence U.S. offensive cyber operations and policies that may affect cybersecurity and defense.

Dual-hat Arrangement¹³: The President should consider a dual-hatting the NCD, or a member of his or her staff, to the NSC in a senior-level position.¹⁴ Such an arrangement would organically and seamlessly integrate the NCD into the national security decision-making process, afford the position a more direct pathway to influence the policy agenda, and make NSC processes more efficient by drawing ONCD resources and expertise. More practically, a dual-hat arrangement would help deconflict and reduce demands on department and agency time by preventing the creation of parallel coordinating structures.

RECOMMENDATION 3

CREATE A NATIONAL CYBER COMMUNITY & NATIONAL CYBER MISSION

Although the NCD was authorized to coordinate among federal departments and agencies and bring greater coherence to the national cyber effort, neither its authorizing statute nor any subsequent Executive Order have defined a core group of agencies under a unified “national cyber mission.” This omission contrasts sharply with similarly structured senate-confirmed positions—the United States Trade Representative (USTR), Office of National Drug Control Policy (ONDCP), and Office of the Director of National Intelligence (ODNI)—whose authority and scope of mission go hand in hand with a designated core group of departments and agencies.¹⁵ In the case of ODNI and ONDCP, this designation entailed the formation of a national-level program—National Drug Control Program or National Intelligence Program—which formed the basis of both positions’ authority for budget review, programmatic guidance, and issuance of national strategy and guidance documents. Lacking such definitions, both the NCD’s remit and the corresponding national cyber mission can be interpreted variably and inconsistently, which undermines the position’s authority, reduces accountability, and perpetuates confusion over roles and responsibilities among the many White House entities involved in cybersecurity.

A key challenge lies in determining a practical and concise scope for the national cyber mission itself—even if limited to cyber defense and security. These issues cut across virtually all agencies, whether as an enterprise-wide concern (most departments), a primary mission (Cybersecurity and Infrastructure Security Agency, National Security Agency Cybersecurity Directorate, U.S. Cyber Command), an ancillary but substantial element of their primary mission (Food and Drug Administration, Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response), or an occasional but essential target of their authorities (Office of Foreign Asset Control sanctions, law enforcement investigations, etc.). If that scope is too narrow, the NCD will lack the authority to engage with all critical players; if too broad, the NCD’s efforts will be diluted by competing interests and mismatched objectives more appropriately handled by existing bodies in separate forums tailored to their interests.¹⁶ As a result, the very cohesion the NCD was designed to provide remains elusive.

To address this gap, Congress should establish a National Cyber Community headed by the NCD and composed of those elements within departments and agencies that bear principal re-sponsibility for securing cyberspace and its foundational technologies. Modeled on the intelligence community (IC), this national cyber community would serve as the NCD’s “core constituency” and would constitute the principal entities with whom it collaborates to coordinate and implement policy, align programs and priorities, and streamline procedures in the pursuit of the defense and security of cyberspace. In a manner similar to the IC, the national cyber community’s “policy” focus would be on procedural and programmatic issues and implementation, reserving broader, strategic issues for the NSC-led process where they are best coordinated and considered in the broader national security context.

Criteria and Designation: The legislation would direct the President, on the recommendation of the NCD in coordination with the head of relevant departments and agencies, to designate as members of the national cyber community elements of departments and agencies whose mission is principally focused on the security and defense of cyberspace or its underlying technological ecosystem. This standard ensures a manageable community size while only including entities that have the programmatic clout and authority necessary to drive meaningful outcomes while allowing for adaptability as missions evolve.

National Cyber Mission: The legislation would formally establish the national cyber mission, composed of the specific programs managed by members of the national cyber community and serving as the foundation for the NCD’s budget review authority. This mirrors existing models, such as ODNI’s National Intelligence Program or ONDCP’s National Drug Control Program, ensuring the NCD can oversee and align resource allocation across its constituent agencies.

Core Mission Distinction: The national cyber community construct draws an intentional line between elements of departments and agencies capable of systemic, national-level impact in the cyber mission—those with the authority, programmatic heft, and budget to influence the security and defense of cyberspace—and those whose focus or authority is more localized, sectoral, limited, or niche in scope (federal cybersecurity, sector risk management, etc.) This framework recognizes that while some departments and agencies may play a crucial supporting role, their impact does not extend systemically.

Representative Leads: The Community should include as members key agencies that lead or coordinate efforts from among interagency groups, such as CISA representing Sector Risk Management Agencies and the Federal CISO representing Federal CISOs, to ensure their priorities can be accounted for collectively while protecting the community’s clarity of focus and cohesion in driving systemic improvements in cyber defense and security.

RECOMMENDATION 4

ESTABLISH YEARLY NATIONAL CYBER PRIORITIES

While a National Cyber Strategy can effectively set high-level priorities that shape medium- and long-term programs, there is a critical gap in mechanisms that can guide the year-to-year annual priorities for operational and programmatic actions within and across federal departments and agencies. The budget process is effective in setting overall programmatic guidance, but does not prescribe specific operational details or concrete plans. Executive orders and presidential memoranda offer powerful instruments for articulating national goals, but they are not consistently updated or applied on a yearly cycle. Meanwhile, the NSC process—the default coordination hub—has limited resources and must address a constant stream of urgent, high-profile national security issues, constraining its ability to proactively drive cyber priorities at a granular level. As a result, operational and programmatic priorities tend to be reactive, shaped by near-term political imperatives, and are prone to shifting without a sustained framework to ensure continuity and long-term strategic alignment.

In the absence of a robust, routinely updated coordination mechanism, the federal government lacks a reliable means to department and agency activity year-to-year. This challenge extends to aligning operational endeavors not only across government entities but also between the public and private sectors, where differing incentives and capabilities further complicate cohesive action. Each agency conceives of its cyber mission differently: some focus on the threat actor (DoD, FBI, the intelligence community), others on the assets requiring protection (DHS, CISA, the Department of Energy), and still others on the technologies most vulnerable to exploitation (CISA, NIST, among others). The result is an operational landscape where collaboration is often *ad hoc* rather than systematic. It is often only in the aftermath of a major incident—when the nature of the threat, the assets at stake, and the relevant technologies all converge—that the political will and mission clarity emerge to drive truly coordinated interagency and public-private collaboration. This reactive model underscores the pressing need for a more deliberate, consistent, and forward-looking approach to operational alignment in cyberspace, one that is institutionalized rather than crisis-driven and that fosters a sustained commitment to shared cybersecurity objectives.

To address the gap between strategic intent and operational alignment, the President should establish yearly national cyber priorities, defining a specific threat actor (or set of actors) along-side the most critical at-risk assets or technologies. These annual priorities would function much like the National Intelligence Priorities Framework (NIPF)—providing a formal, recurring process through which the government can coordinate and adjust its cyber efforts in a structured, forward-looking manner.¹⁷ By identifying in advance the intersection of threat, asset, and technology, the framework would recreate clarity of purpose and objective in a crisis response, but without waiting for an incident to trigger unified action. This role is consistent with the NCD's authorizing statute, which directs the NCD to “develop for the approval of the President...operational priorities, requirements, and plans.”¹⁸

Foundational Framework: Yearly cyber priorities would merely serve as a foundational framework of shared priorities—a baseline that enables coordination without constraining the NSC's or the President's prerogative to shift focus in response to evolving threats or strategic shifts. Such a process would preserve the NSC's prerogative while offering a common language and framework for agencies. The NSC could still pivot rapidly to emerging crises or geopolitical shifts, as needed.

Formation of Priorities: The NCD would oversee a structured process in coordination with relevant federal departments and agencies. This process would establish the foundational framework, nominate key priorities, rank their significance, and culminate in the submission of recommendations to the President for final approval. Select priorities once approved should be shared publicly to foster alignment between public and private sector efforts.

Inform Interagency “Campaigns”: Priorities should serve as the basis for “campaigns,” marshaling departmental authorities to defend against and disrupt threat actors. By uniting legal, policy, and enforcement tools, these multi-agency efforts can deny adversaries the ability to exploit vulnerabilities in target-ed technologies or infrastructure. Coordinated campaigns can also safeguard critical assets, ensuring that each department's mission is nested within the broader national cyber strategy.

Industry and Ally Alignment: These annual priorities would allow industry and allies to self-align with federal efforts. Clear, predictable signals on the threats and assets at the center of U.S. attention make it easier for private sector stakeholders and international partners to adjust their own risk management, incident response, and collaboration activities.

RECOMMENDATION 5

CODIFY AND STRENGTHEN THE JOINT COLLABORATIVE ENVIRONMENT

In 2022, CISA established the Joint Collaborative Environment (JCE) to serve as a government-wide information-sharing platform, intended to enable the exchange of cyber threat, risk, and vulnerability data among federal agencies and private-sector stakeholders. The JCE was inspired by the Cyberspace Solarium Commission (CSC), which first recommended the creation of the JCE in its 2021 report. Both the CSC and CISA viewed the JCE as a critical means to achieve shared situation awareness and early detection of emerging threats through real-time data sharing and analytic collaboration across departments and agencies and between the public and private sectors.

However, CISA's implementation of the JCE is missing a critical piece. The CSC's original proposal divided the initiative into two critical elements: the JCE platform itself, and a White House-led "Cyber Threat Data Standards and Interoperability Council."¹⁹ The council would identify participating agency programs, address barriers to interoperability, and recommend budget adjustments to overcome technical hurdles to information sharing. Designed to ensure interagency buy-in—especially critical given the historical reluctance of departments and agencies to share operational data—the council is a vital element to create the downward pressure needed to drive meaningful collaboration.

The success of any information-sharing or social platforms like the JCE, depends on network effects—a virtuous cycle where participation increases value and in turn further incentivizes participation. These platforms require achieving a "critical mass" of value to start that cycle—a serious challenge if CISA must rely solely on its own limited threat intelligence. Given the underwhelming performance of previous initiatives such as automated indicator sharing (AIS)²⁰, where participation and shared indicators declined over time, there are significant reasons to doubt whether CISA alone can provide the compelling value proposition necessary to both attract a broad user community and overcome the parochial interests and procedural intransigence that have thus far characterized interagency cyber threat information sharing. Without a formal mechanism to encourage—or require—agency involvement, CISA may continue to face an uphill struggle in building a critical mass of users and value that spurs the type of self-reinforcing collaboration needed for the program to be successful.

To address this gap, Congress should formally codify the Joint Collaborative Environment and the Cyber Threat Data Standards and Interoperability Council ("Council") into law. Modelled after the "Cyber Threat Information Collaboration Environment" provision included in a proposed floor amendment to the National Defense Authorization Act for 2023, the law would direct the council, chaired by the NCD and composed of the Secretary of Homeland Security, DNI, and Secretary of Defense (or designated representatives), to establish data standards, requirements for interoperability, and identify and designate programs that shall participate or be made interoperable with the JCE. This arrangement is intended to improve the chances of interagency buy-in, thereby "jumpstarting" the JCE's utility and ensuring the platform's long-term viability.

National Security Agency Involvement: In certain iterations of the legislation, the National Security Agency (NSA) played a central role, co-developing and managing the JCE in partnership with CISA. This was intended to bring to bear the NSA's technical expertise and significant experience in managing sensitive, large-scale, data environments with sophisticated access controls.

Phased Implementation: The key priority of the JCE should be first reducing barriers to sharing between departments and agencies who routinely collect or acquire cyber threat data or data relevant to cyber threat analysis—then inclusion of the private sector. This has the advantage of allowing the government space to work through some of the most significant hurdles preventing interagency sharing while increasing the value proposition—and incentive—for private sector involvement when such hurdles have been overcome.

Privacy and Data Governance: The council shall establish a committee composed of the privacy officers of the principal members who will be responsible for developing robust data governance structures and procedures to ensure the protection of sensitive data, compliance with federal regulations and statutes, and adherence to existing agreements with private sector entities.

Non-profit Clearinghouse: While the JCE has a direct path to reduce roadblocks in information sharing between federal departments and agencies, there are still significant complexities, costs, and disincentives that may be in play that complicate private sector participation. Congress may want to consider the benefits of designating and funding a non-profit to serve as a clearinghouse or non-government "integrator" that would act as an operating partner with CISA. This would help legally and institutionally address some of the perceived risks associated with sharing information directly with the federal government.²¹

RECOMMENDATION 6

CREATE A CYBERSECURITY REGULATORY HARMONIZATION COUNCIL

The U.S. cybersecurity regulatory landscape is best characterized as “federated”, where, in the absence of a national-level preemptive cyber law, each independent and executive branch regulatory agency, as well as each state and local government, is empowered to promulgate regulations within its jurisdiction as it sees fit.²² The past five years have witnessed a surge in cybersecurity-focused regulations from authorities across all sectors and echelons²³ resulting in an increasingly complex patchwork of compliance requirements, often with conflicting, overlapping, or duplicative mandates. Companies operating in heavily regulated sectors, or who are subject to multiple regulatory authorities, face an increasingly complex maze of rules, leading to significant costs and inefficiencies. In response to the ONCD’s 2023 Request for Information (RFI) on cybersecurity regulatory harmonization, companies emphasized that the fragmented regulatory approach often mean diverting critical resources from security programs to compliance activities—resulting in the adoption of a checklist-based approach to cybersecurity rather than maintaining tailored risk management programs.²⁴

A significant contributing factor to this issue is the lack of any mechanism with the necessary authority to coordinate and deconflict among the U.S.’s diverse array of regulatory authorities. The President is limited in the power to compel either independent regulatory agencies or state and local authorities to conform to a common standard. While the Office of Information and Regulatory Affairs (OIRA) plays a significant role in coordinating (non-independent) agency rulemaking ahead of publication in the Federal register, it was neither designed for nor is it well-suited to develop and enforce harmonized regulatory standards across agencies. Existing executive branch efforts, like the Cybersecurity Forum for Independent and Executive Branch Regulators, while well-intended, are voluntary, have varied wildly in activity over time, and have lacked the sustained attention, momentum, and political force necessary to make significant headway in this space.²⁵ This has resulted in a fragmented and inefficient regulatory environment, where agencies often act in isolation, leading to a proliferation of overlapping and inconsistent requirements.

To rectify these issues, Congress should codify into law a Cybersecurity Regulatory Harmonization Council within the White House, chaired by the NCD, and composed of both executive branch and independent regulatory agencies.²⁶ Modeled on the approach outlined in the *Streamlining Federal Cybersecurity Regulations Act*, the council would have the primary goal of developing and implementing a cohesive, comprehensive, and streamlined approach to cybersecurity regulation.²⁷ This includes the creation of a common lexicon of cyber regulatory terms, development of a single, unified framework for applying cybersecurity standards, and ensuring that regulations are risk-based, outcome-focused, and aligned with consensus standards like the NIST Cybersecurity Framework. This council must also have the power to review and harmonize existing regulations, as well as ensure that any new regulations are consistent with the broader national cybersecurity strategy and avoid duplication.

Adaptable and Tiered Framework: The regulatory structure developed by the council should be adaptable across agencies, considerate of sector-specific needs, and built around a tiered model that considers the common risk profiles of entities with respect to size, business model, criticality, and potential consequences of their disruption. Such an approach ensures that cybersecurity requirements are proportionate to an organization’s operational context and scaled to its size, improving overall effectiveness without imposing undue burdens.

Yearly Report: The council should submit a yearly report to Congress detailing its activities, progress in harmonization efforts, and recommendations for legislative or regulatory changes. This report would provide transparency, ensure accountability, and allow for ongoing Congressional oversight of the council’s work.

Third-Party Service Providers: The council should also seek to address regulatory discrepancies that burden third-party service providers, such as cloud services. Although these firms are not always directly regulated, they often contend with a maze of overlapping and contradictory requirements imposed indirectly by the regulatory burden born by their customers. By harmonizing and streamlining these rules, the council can foster a more coherent and efficient environment that benefits both service providers and the regulated entities they support.

State-level Regulation: While the council is limited to the degree it can influence state-level regulation, it should develop its framework and harmonization efforts as a model that states are able to adopt in the long-term. This approach will not solve the problem of conflicting state-level regulations, immediately, but it should reduce potential barriers to states conforming to the harmonized federal framework as new rules are developed and promulgated.

ENDNOTES

- 1 U.S. Cyberspace Solarium Commission, *Cyberspace Solarium Commission Final Report*, March 2020, solarium.gov, https://drive.google.com/file/d/1ryMCIL_dZ30QyJfQkFf10MxIJGT4yv/view; For additional context on Cyberspace Solarium Commission intentions and objectives for the position, see John Costello and Mark Montgomery, “How the National Cyber Director Position Is Going to Work: Frequently Asked Questions,” *Lawfare*, February 24, 2021, <https://www.lawfaremedia.org/article/how-national-cyber-director-position-going-work-frequently-asked-questions>
- 2 Interviews with current and former ONCD officials are consistent with media reports on the continuing uncertainty and lack of clarity with respect to ONCD roles and responsibilities in the Executive Office of the President. For a more comprehensive assessment, see Ari Schwartz, Inés Jordan-Zoob, and Samara Friedman, “Through the Looking Glass: An Updated Vision for the Office of the National Cyber Director,” Center for Cybersecurity Policy and Law, <https://dd80b-675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn.com/external/67589ea3f1a160cf31996f8cccpl-oncdfinal.pdf>
- 3 Natasha Bertrand, “Biden Taps Intelligence Veteran for New White House Cybersecurity Role,” *Politico*, January 6, 2021, <https://www.politico.com/news/2021/01/06/biden-white-house-cybersecurity-neuberger-455508>.
- 4 The initial draft of the National Cyber Director statute was heavily modified, for example, to address concerns by the Trump Administration that the position’s policymaking and Presidential advisory role would encroach upon the authority of the National Security Advisor. The result was a shift in language from the NCD advising the President on cybersecurity issues generally to advising the President on “the coordination” of these issues—a small but significant distinction.
- 5 These positions include the U.S. Trade Representative (USTR, created in 1974), the Director of the Office of Science and Technology Policy (OSTP, 1976), and the Director of National Drug Control Policy (ONDCP, created in 1988). Cyberspace Solarium Commission drew lessons and inspiration from the Director of National Intelligence (DNI, created in 2004) but it did not directly serve as a model in outlining the position’s responsibilities in statute.
- 6 For a fuller understanding of the authorities of the National Cyber Director and what they mean both legally and practically within the White House, see Devin DeBacker’s excellent analysis in *Lawfare*: Devin DeBacker, “How the President Can Shape the Role and Oversight of the National Cyber Director,” *Lawfare*, December 6, 2021, <https://www.lawfaremedia.org/article/how-president-can-shape-role-and-oversight-national-cyber-director>
- 7 For example, the U.S. Trade Representative was created in the *National Trade Act of 1974* and was clarified by Executive Order 11846 “Administration of the Trade Agreements Program” in 1975. Director of National Drug Control Policy was created by the *Anti-Drug Abuse Act of 1988* and clarified by Executive Order 12564 “
- 8 Barack Obama, “Presidential Policy Directive 41 -- United States Cyber Incident Coordination,” July 26, 2016, <https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>.
- National Security Council, “Vulnerabilities Equities Policy and Process for the United States Government,” November 15, 2017, <https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF>.
- 10 The Cyber Safety Review Board is an interesting example of a policy change that needs an update to account for the NCD. At the time the CSRB was conceived, the ONCD was not a viable host for the organization—having just been signed into law. The need for the CSRB to be objective in assessing root causes of incidents and identifying areas of improvement in their response and handling argues strongly for the board to be moved from DHS and CISA—who are often directly involved in the handling of incidents that are likely to come before the board. Joseph R. Biden Jr., “Executive Order on Improving the Nation’s Cybersecurity,” May 12, 2021, <https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>
- 11 A more permanent solution to the status of the Federal CISO would be codifying a dual-hat arrangement into law or by realigning Federal cybersecurity responsibilities more broadly among CISA, OMB, and ONCD—both of which lay outside the scope of this paper.
- 12 Specifically, the NCD authorizing statute directs the NCD to “lead coordination of the development and ensuring implementation by the Federal Government of integrated incident response to cyberattacks and cyber campaigns of significant consequence, including... support for the integration of defensive cyber plans and capabilities with offensive cyber plans and capabilities in a manner consistent with improving the cybersecurity posture of the United States”; See 6 U.S.C. § 1500 (c)(1)(D).
- 13 When crafting the responsibilities of the position of National Cyber Director, the Cyberspace Solarium Commission designed the role with a dual-hat arrangement in mind. The commission recognized that of the senate-confirmed positions in the White House, the NCD would be unique in the degree that its primary work involves elements of national security. The commission viewed the NCD as a continuation, restoration, and strengthening of the former NSC Cybersecurity Coordinator position after its abolishment by President Trump in 2018; however, given limitations on Congress’s legislative ability to restore that role in the NSC, the creation of a senate-confirmed position was the most practical pathway to ensure that the cybersecurity coordinator position would continue in some form and be insulated from Presidential caprice. Though it could not be prescribed in law, a dual-hat arrangement was seen as a logical means by which the President could fully align the NCD within the national security apparatus of the NSC.
- 14 Dual-hatted roles between the NSC and senate-confirmed offices within the White House are not uncommon. Notably, Grant Schneider served as both Federal CISO and Senior Director for Cyber on the NSC and Jason Matheny served as both the Deputy Director for National Security in OSTP and as a “coordinator” in the NSC. These arrangements, however, are arrived at by convention and agreement on an ad hoc basis and not established as permanent fixtures in the organization of the Executive Office of the President. See Jason Miller, “Schneider Leaving Federal CISO Role for Private Sector,” *Federal News Network*, August 17, 2020, <https://federalnewsnetwork.com/people/2020/08/schneider-leaving-federal-ciso-role-for-private-sector/> and Bob Davis, “Jason Matheny on Tech, National Security and China,” *The Wire China*, February 18, 2024, <https://www.thewirechina.com/2024/02/18/jason-matheny-on-tech-national-security-and-china/>.
- 15 Although the DNI didn’t serve as an institutional model for the NCD—given it’s not a Senate-confirmed White House position—it did provide a functional blueprint. Both roles aim to coordinate elements of departments and agencies that, while retaining their own missions and authorities, share a set of similar or common disciplines and face overlapping informational, operational, and programmatic interdependencies.
- 16 For a more rigorous study of the considerations that go into the size, makeup, and structure of a stakeholder group in a deliberative process, see Tomas M. Koontz and Elizabeth Moore Johnson, “One Size Does Not Fit All: Matching Breadth of Stakeholder Participation to Watershed Group Accomplishments,” *Policy Sciences* 37, no. 2 (June 2004): 185–204.
- 17 Director of National Intelligence. *Intelligence Community Directive 204: National Intelligence Priorities Framework (NIPF)*. Washington, DC: Office of the DNI, January 2015.
- 18 6 U.S.C. § 1500 (c)(1)(E)
- 19 U.S. Cyberspace Solarium Commission, *Cyberspace Solarium Commission Final Report*, March 2020, solarium.gov, https://drive.google.com/file/d/1ryMCIL_dZ30QyJfQkFf10MxIJGT4yv/view.
- 20 Interviews and roundtables with current and former govern-

ment officials revealed a general skeptical view of the JCE and CISA's associated Cyber Analytic and Data System (CADS)—opinions admittedly colored by a negative perception of CISA's track record on information sharing programs. See Department of Homeland Security Office of Inspector General, "CISA Faces Challenges Sharing Cyber Threat Information as Required by the Cyber-security Act of 2015," September 25, 2024, <https://www.oig.dhs.gov/sites/default/files/assets/2024-09/OIG-24-60-Sep24.pdf>.

21 The notion of non-profit or non-government, designated information sharing clearinghouses has long been discussed. See Jason Healey, *Breaking the Cyber-Sharing Logjam* (Washington, DC: Atlantic Council, 2015), https://www.files.ethz.ch/isn/188937/AC_BreakingCyber-SharingLogjam_WEB-1.pdf

22 It should be noted, here, that cybersecurity joins digital privacy as an area of law where in the absence of a preemptive Federal authority state, local, and Federal regulators have created a complex, overlapping web of requirements that is both costly and by its nature disharmonized. The simplest and most elegant solution in both cases would be the establishment of a national-level, preemptive statutory authority under a "dual regulatory" model with state and sector regulators—but that path is likely politically and practically unviable.

23 For a summary of cybersecurity regulation and related harmonization initiatives, see U.S. Government Accountability Office. *Cybersecurity: Efforts Initiated to Harmonize Regulations, but Significant Work Remains*. GAO-24-107602. Washington, D.C.: June 5, 2024. <https://www.gao.gov/assets/gao-24-107602.pdf>

24 For a summary and consolidation of RFI responses, see Office of the National Cyber Director. *Summary of the 2023 Cybersecurity Regulatory Harmonization Request for Information*. June 2024. <https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn.com/external/cybersecurity-regulatory-harmonization-rfi-summary-oncd-1.pdf>.

25 Chris Jaikaran, "Harmonic Dissonance—Synching Up Cybersecurity Regulations," Congressional Research Service Insight, July 31, 2023, https://www.everycrsreport.com/files/2023-07-31_IN12211_5419339f79cbe4e60191148118b8307f494e31a4.pdf.

26 For an excellent deep-dive on the drivers of regulatory disharmony, see Jason Healey and Samuel Dab, "Drivers of Disharmony in U.S. Cyber Regulations," Lawfare, December 18, 2024, <https://www.lawfaremedia.org/article/drivers-of-disharmony-in-u.s.-cyber-regulations>. For a better understanding of key areas where cybersecurity regulation faces conflicting standards and requirements, see Josephine Wolff, "Harmonizing U.S. Cybersecurity Regulations: Opportunities & Challenges," SSRN Scholarly Paper, November 30, 2024, <https://ssrn.com/abstract=5044551>.

27 U.S. Congress, Senate, *Streamlining Federal Cybersecurity Regulations Act*, 118th Cong., 2d sess., S. 4630, re-reported in Senate December 2, 2024, <https://www.congress.gov/118/bills/s4630/BILLS-118s4630rs.pdf>.