JANUARY, 2025

CYBERSECURITY POLICY RECOMMENDATIONS FOR THE NEW ADMINISTRATION

With an ambitious suite of goals for your Administration under consideration, we want to offer our recommendations and assistance with one set in particular: the party platform's commitment to "use all tools of National Power to protect our Nation's Critical Infrastructure… and raise the Security Standards for our Critical Systems and Networks and defend them against bad actors."

The cyber risks facing America present short and long-term challenges. Cyber crooks, rogue nation states, and terrorists often see the first 100 days of a new Administration as a prime opportunity to attack during a time of transition. Both U.S. government data and America's companies are at risk. As past incidents demonstrate, there is potential for disruption to our way of life: from mass theft of government employees' personal information, to lines at the pump, to infrastructure security risks like Chinese military hackers in our water supply. These threats present your Administration and Congress with a key window in which to act.

At the Aspen Cybersecurity Program, we do not just 'admire problems.' Instead, we have built a robust and bipartisan coalition dedicated to addressing critical issues and finding solutions. We work with top talent of current and former government officials as well as leaders of industry across multiple sectors: including tech, telecommunications, manufacturing, retail, and defense. During the first Trump Administration, we were honored to work closely with federal law enforcement, the U.S. Intelligence Community, and others to find solutions.

The Aspen Institute's US Cybersecurity Group stands ready to help your Administration tackle its cybersecurity goals. Whether it's offering your new team a sounding board, supporting important work in Congress, or getting input from an array of industry leaders, we look forward to supporting the work ahead in this area.

We recommend a few first steps for your consideration and further discussion:

1) PERSONNEL IS POLICY: DEMONSTRATE CYBERSECURITY LEADERSHIP AND PREPARE FOR IMMEDIATE RESPONSE

Streamline cybersecurity leadership; White House cyber components as well as federal departments and agencies with critical cybersecurity responsibilities are not organized efficiently. Redundancies, delayed appointments and vacant political positions can make it hard to develop coordinated and unified strategies, policies and response efforts. You and your advisors have an opportunity to prioritize, clarify, and align roles to promote efficiency, economies of scale, and maximum impact.

2) PRIORITIZE CYBERSECURITY REGULATORY ALIGNMENT AND STREAMLINING

Streamline regulations; there are too many and they are inconsistent. In your first Administration, you prioritized cutting burdensome regulations; in your second Administration, we recommend doing the same in cybersecurity policy. Prior reports have identified dozens of overlapping regulations and approaches that can waste resources and a balance must be struck between centralization and customization in terms of standards and regulation. In the Trump Administration, all new requirements must be rationalized around simple core principles that appropriately balance national security and business interests, including small businesses and local governments. In this post-Chevron era, working with Congressional leadership will be critical.

3) PARTNER WITH THE PRIVATE SECTOR TO PROTECT CRITICAL INFRASTRUCTURE AND HOLD BAD ACTORS ACCOUNTABLE

The current state of U.S. infrastructure vulnerability is unacceptable. Power grids, transportation systems, water supplies, and communication networks are all in jeopardy. You can send a clear message: the United States will defend itself against cyber aggression with the same resolve as it defends against physical threats. Everything from defensive measures to offensive operations should be on the table. Crooks, spies and terrorists should be hunted jointly with key private sector actors. Efforts to "defend forward" must be continued in conjunction with providing resources and assistance to critical, often overlooked entities such as small businesses and rural communities. Further, we must leverage the U.S.'s unique combination of innovation and capital investment to support and incentivize in areas of the world aligned with U.S. interests.

4) CONTINUE BUILDING MECHANISMS TO MEASURE PROGRESS

Government efficiency depends on good data and clear-eyed analysis. We can't understand what works without data. We need a repository of data in this area to know what to keep and what to cut.

5) RESET THE DISCUSSION WITH IMPROVED COMMUNICATIONS AROUND CYBERSECURITY ISSUES

The White House has the world's greatest megaphone. Using the White House bully pulpit is essential so that the American people know the stakes in cybersecurity and what steps they can take to be part of solutions. For too long we have been discussing these commonly agreed-upon cyber strategies with limited progress. To move forward quickly, it is imperative to advance a new understanding of cybersecurity from a technology problem for technologists to solve; to an issue of national concern that requires an all-hands-on-deck approach. Cybersecurity must be seen as what it is: 1) a key enabler of economic growth and national security and 2) a critical tool in the effort to counter nation state actors like China.

> **Our network is prepared to help move these priorities forward, including the launch of onboarding sessions for new government leaders. These sessions, led by industry leaders, will focus on understanding the current state of the critical pillars of cybersecurity, the authorities and constraints of each department and agency, and best practices for moving the above priorities forward.**

We look forward to hearing from you and your team and continuing the work.

ACKNOWLEDGEMENTS

This document is authored by the Aspen Institute's US Cybersecurity Group members who brought forward their ideas and recommendations for Aspen Cyber staff, experts, and our advisors resulting in the above. These recommendations would not be possible without their deep experience across the public and private sector gained over decades and that continue to critically challenge how we improve cybersecurity and cybersecurity policy.

SIGNED,
THE ASPEN INSTITUTE'S US CYBERSECURITY GROUP

The Aspen Institute's US Cybersecurity Group is the leading cross-sector, public-private forum for promoting a secure future for America's institutions, infrastructure, and individuals—in cyberspace and beyond.