

STRATEGIC OBJECTIVE #3:

**INTEGRATE PUBLIC- AND PRIVATE-SECTOR CYBER DEFENSE EFFORTS**

The U.S. government should improve its capacity to better coordinate its own cyber defense planning and operations and integrate its operations with the private sector. Current federal government operations to defend against cyberattacks are decentralized and tend to be uncoordinated, leading to inefficiencies and the lack of a coherent, strategic approach to defend the nation. Therefore, the interests of critical infrastructure providers and parts of the private sector that are key to cyber defense are not always adequately incorporated into these defensive operations because of a lack of institutionalized processes and procedures for collaboration with federal agencies and a dearth of threat information.

*Key Recommendation*

**5.3 Congress should direct the executive branch to strengthen a public-private, integrated cyber center within CISA in support of the critical infrastructure security and resilience mission and to conduct a one-year, comprehensive systems analysis review of federal cyber and cybersecurity centers, including plans to develop and improve integration.**

Over the past decade, the U.S. government has stood up a number of missions, centers, and programs across the federal government to strengthen U.S. cybersecurity. As the number of agencies involved in the cybersecurity mission has expanded, however, there have been difficulties in integrating their operations for coordinated action, common situational awareness, and joint analysis, and the risk of fragmented, uncoordinated efforts has grown. U.S. public-private cybersecurity efforts will continue to be undermined without effective, meaningful cooperation across federal departments and agencies. While the recommendations in this report that call for investment in programs that support and enable joint planning, coordinated action, and shared information and analysis—all vital parts of operational collaboration—can do much to address these issues, they are insufficient if underlying structural procedural issues remain unaddressed. More importantly, these recommendations are no substitute for human-to-human collaboration and close, trusted relationships. For the United States, seamless collaboration means diminishing barriers between agencies and between the public and private sectors with a focus on relationships—underpinned and served by a

strong technical foundation like the Joint Collaborative Environment (recommendation 5.2).

CISA is already a key component in coordinating the cyber defense and security efforts of federal departments and agencies and integrating these efforts with the private sector. Initially conceptualized through a national cybersecurity and communications integration center (NCCIC), the vision for CISA's cyber mission is to be the U.S. government's primary coordinating body charged with forging whole-of-government, public-private collaboration in cybersecurity. However, CISA has been institutionally limited in its ability to fully carry out this mission, hindered by inadequate facilities, insufficient resources, lack of buy-in from other federal departments and agencies, ambiguity from Congress on its role and position in relation to other agencies, and inconsistent support to and integration with the private sector. To truly operationalize cybersecurity collaboration with the private sector, the U.S. government must strengthen an integrated cyber center within CISA, improve its connectivity with other key cyber and cybersecurity centers—including the FBI's National Cyber Investigative Joint

Task Force (NCIJTF), ODNI's Cyber Threat Intelligence Integration Center (CTIIC), DOD's Integrated Cyber Center and Joint Operations Center (ICC/JOC), and NSA's Cybersecurity Directorate (CSD)—and ensure that the systems, processes, and *human element* of collaboration and integration are fully brought to bear in support of the critical infrastructure cybersecurity and resilience mission.

Congress should direct the executive branch to immediately begin to strengthen a public-private, integrated cyber center within CISA in support of the critical infrastructure cybersecurity and resilience mission and in coordination with centers in the FBI, ODNI, and DoD. While this is under way, the executive branch should conduct a one-year, comprehensive systems analysis review of federal cyber and cybersecurity centers, which should include developing plans to better integrate the centers. The review should identify challenges and solutions to more effectively integrate elements of federal cyber centers, the private sector, and CISA with a view toward reinforcing human-to-human collaboration, reducing procedural or technical barriers to integration, implementing other recommendations within this report, and, to the greatest extent possible, increasing meaningful integration of cybersecurity stakeholders. This process should be undertaken by the National Cyber Director (recommendation 1.5), or, in lieu of a National Cyber Director, a working group led by DHS, in coordination with DoD, DOJ, FBI, and ODNI. In particular, this review should address the following actions.

*Strengthening CISA's Public-Private Integrated Cyber Center:* CISA's role as the primary interface between the federal government and critical infrastructure for cybersecurity places it in a unique position to operationalize the type of public-private collaboration necessary to secure and defend cyberspace and the critical infrastructure that relies on it. In strengthening a public-private integrated cyber center within CISA, the executive branch should identify continuing gaps and shortcomings in CISA's current capacity, structure, funding, and integration

of its work with sector-specific agencies that prevent it from fulfilling its role as the central coordinator among federal centers for critical infrastructure cybersecurity and resilience.

*Identifying Areas of Integration and Collocation:* The executive branch should assess areas where existing federal cyber centers, or portions of a center's mission, would benefit from greater integration or collocation to support cybersecurity collaboration with critical infrastructure. The review should identify and acknowledge continuing gaps and shortcomings in associated capacity and funding of the FBI and ODNI, identify methods to better integrate efforts with CISA in support of its mission to ensure the security and resilience of critical infrastructure, and identify where federal agencies have distinct statutory authorities (i.e., those of law enforcement, counterintelligence, military, and intelligence operations) best kept distinct and separate from these efforts.

*Supporting the National Security Agency's Cybersecurity Directorate (CSD):* The executive branch review of federal cyber centers should include a particular focus on NSA's new Cybersecurity Directorate. Sustaining and strengthening the CSD's collaboration with and support to other federal departments and agencies, particularly CISA, is critical in ensuring that the U.S. government's technical expertise and intelligence resources are fully brought to bear in supporting both federal and public-private cybersecurity efforts. The executive branch should identify continuing gaps and opportunities for greater integration of CSD with CISA, other federal cyber centers, and, as needed, the private sector in its role of securing national security systems.

*Assessing Centralized, Collocated Public-Private Collaboration:* The U.S. government should identify lessons from the United Kingdom's National Cybersecurity Center model, which maintains collocated classified and unclassified environments for private-sector cybersecurity integration. The review should assess whether an integrated cyber center within CISA should be similarly

organized into two environments: an unclassified side, which handles general cybersecurity coordination and cooperation with the private sector, and a classified side with appropriate support from CSD, which handles deeper collaboration with systemically important critical infrastructure and the intelligence community on systemic cyber security and resilience and cyber defense operations. The executive branch should assess continuing gaps and limitations in its ability to provide for greater centralization of public-private cybersecurity efforts similar to the NCSC model within a CISA integrated cyber center.

*Increasing Public- and Private-Sector Integration:* The executive branch review should also recommend procedures and criteria for increasing and expanding the participation and integration of public- and private-sector personnel into U.S. government cyber defense and security efforts. This review should identify continuing limitations or hurdles in the security clearance program for private

sector partners and in integrating private sector partners into a CISA integrated cyber center, including integrating private sector organizations like information sharing and analysis centers (ISAC) and the Financial Systemic Analysis and Resilience Center (FSARC).

Within one year and upon the conclusion of its review, the executive branch should report its findings to Congress and provide recommendations on additional resources or authorities required to implement its plans and to address gaps the review has identified. The executive branch will conduct an annual review thereafter, providing a yearly report to Congress on the status of its efforts, any revised findings or additional resources or authorities required, and its progress in addressing the areas identified in this recommendation. Future reports should include updates on the progress of the Joint Collaborative Environment (recommendation 5.2) in enabling greater federal agency and public-private integration, after the environment comes online.

### Key Recommendation

#### **5.4 The executive branch should establish a Joint Cyber Planning Cell under the Cybersecurity and Infrastructure Security Agency to coordinate cybersecurity planning and readiness across the federal government and between the public and private sectors for significant cyber incidents and malicious cyber campaigns.**

Successfully defending against malicious cyber incidents, mitigating their consequences, and countering adversary cyber campaigns requires the United States to be able to mount its own coordinated, timely, whole-of-government, public-private cyber defense and security campaigns. Planning is a critical element in fulfilling this mandate. Effective cyber planning ensures that the government both aligns and readies the full range of U.S. government tools in cyberspace and coordinates jointly with private-sector entities, so that they can be employed and integrated seamlessly in response to or in advance of a crisis. Elements of the U.S. government and the private sector, working within their respective sectors

or as individual firms or agencies, often lack the power to independently counter and mitigate a coordinated nation-state cyber campaign. Given this reality, planning is fundamental to enabling and strengthening feedback loops for identifying an effective division of effort and preparing individual agencies and firms to execute responses quickly and with a common understanding of roles, responsibilities, and courses of action.

But efforts to date have not adequately included private-sector stakeholders, and they have been reactive to individual incidents rather than being comprehensive and forward-looking. This inadequate response is largely