

Congress should extend existing law enforcement administrative subpoena authority, currently defined under 18 U.S. Code § 3486, for the Federal Bureau of Investigation and the United States Secret Service to include violations of the Computer Fraud and Abuse Act, 18 U.S. Code § 1030.

Congress should pass the Cybersecurity Vulnerability Identification and Notification Act of 2019 to grant tailored authority to the Director of the Cybersecurity and Infrastructure Security Agency (CISA) to serve administrative subpoenas so that the owners of online systems with known vulnerabilities can be identified, enabling asset response activities and preventing future intrusion.

STRATEGIC OBJECTIVE #2:

IMPROVE COMBINED SITUATIONAL AWARENESS OF CYBER THREATS

The U.S. government should improve combined situational awareness of cyber threats to better support its own and private-sector cyber defensive efforts. For the better part of a decade, expanding public-private collaboration in cybersecurity was synonymous with sharing threat information. Information sharing is an important part of public-private collaboration, certainly, but it is not an end in and of itself. Rather it enables better situational awareness of cyber threats, which can then inform the actions of both the private sector and the government. Truly shared situational awareness is the foundation on which operational collaboration is built and enabled. The U.S. government should leverage its unique, comparative advantages to improve the national collective understanding of the threat, including the information available to the intelligence community and a capacity to integrate information from disparate sources—both public and private. Similarly, the U.S. government must create the structures and processes to work with private-sector entities that have unique insights of their own and a different, and in some cases more comprehensive, view of threats impacting domestic critical infrastructure.

*Key Recommendation*

**5.2 Congress should establish and fund a Joint Collaborative Environment, a common and interoperable environment for the sharing and fusing of threat information, insight, and other relevant data across the federal government and between the public and private sectors.**

While the U.S. government has taken a number of steps to develop situational awareness in cyberspace, there continue to be significant limitations on its ability to develop a comprehensive picture of the threat. Federal departments and agencies each maintain a number of programs that can provide insight into threats affecting U.S. government networks and critical infrastructure. However, the data or information is not routinely shared or

cross-correlated at the speed and scale necessary for rapid detection and identification. This fragmented approach presents further challenges in integrating with the private sector, both as a contributor to and as a beneficiary of U.S. government insight, causing confusion and adding significant burden for the private sector in public-private information-sharing efforts. The U.S. government must take steps to shift the burden of integration onto itself,

establishing the mechanisms and enforceable procedures to build the situational awareness necessary for its own operations and for forging true operational collaboration with the private sector.

To that end, Congress should establish a “Joint Collaborative Environment”, a common, cloud-based environment in which the federal government’s unclassified and classified cyber threat information, malware forensics, and network data from monitoring programs are made commonly available for query and analysis—to the greatest extent possible.<sup>293</sup> Initial stages will focus on the integration of programs across the federal government and with owners and operators of systemically important critical infrastructure, while subsequent phases will focus on extending this environment to larger constituencies of critical infrastructure, including ISACs. This program would make real the promise of a “whole-of-government” and public-private approach to cybersecurity, ensuring that network data, cyber threat intelligence, and malware forensics from each department or agency and the private sector are available at machine speed for comprehensive detection and analysis. The Joint Collaborative Environment should support federal cyber centers, an integrated cyber center at CISA (recommendation 5.3), and a planning cell under CISA (recommendation 5.4).

*Design, Development, and Planning:* Given the complexity of such a program, Congress should allow for a multiyear design and development cycle that proceeds in phases. Initial phases should focus on designing appropriate interoperable standards, affording for integration of all covered data programs, and ensuring that disparate databases or centers can be compatible and interoperable at machine speed and scale. Subsequent phases should focus on sharing high-level insights and more exquisite data—as well as addressing challenges introduced by wider inclusion of private-sector partners.

*Program Management:* Congress should designate DHS and the NSA to act as the primary program managers and

lead agencies charged with developing and maintaining the environment in unclassified and classified space, respectively. Where feasible, unclassified data should be routinely mirrored to a classified environment, and integrated with classified data, to provide enrichment, to broaden context, and to inform and enable indications and warning. Analytic tools should be deployed across classification levels to leverage all relevant data sets as appropriate.

*Designation of Programs:* Congress should direct the executive branch to designate, as part of the environment’s development process and on a routine basis after it is fully operational, federal programs required to participate, feed into, and/or be interoperable with the environment. These federal programs should include any programs that generate, collect, or disseminate data or information in the detection, identification, analysis, and monitoring of cyber threats, such as:

- Government network-monitoring and intrusion detection programs.
- Cyber threat indicator-sharing programs.
- Government-sponsored network sensors or network-monitoring programs for the private sector or for state, local, tribal, and territorial governments.
- Incident response and cybersecurity technical assistance programs.
- Malware forensics and reverse-engineering programs.

*Information-Sharing Protections:* The law should direct that any private-sector information-sharing programs participating in the Joint Collaborative Environment are extended protections analogous to those afforded by the Cybersecurity Information Sharing Act of 2015. The availability of data within this environment is contingent on these protections. When appropriate, the environment will share raw, anonymized data to inform the work of the Bureau of Cyber Statistics (recommendation 4.3), in compliance with that bureau’s charter.

*Data Standardization and Interoperability:* Congress should direct the executive branch to establish an interagency council, chaired by the program managers,

that sets data standards and requirements for program participation and interoperability. Data standards and interoperability requirements should be formed in a public-private process to ensure the full inclusion of the private sector in program design. Membership should include any department or agency that oversees participating, designated programs. The council would be empowered to recommend budgetary changes necessary for programs to make technical or operational adjustments required for integration and interoperability, to establish and maintain the environment, and to ensure that the environment has adequate security to prevent breaches and to guard against and detect false data insertion.

*Modules and Tooling:* Congress should appropriate necessary funds to DHS and the NSA to develop, purchase, and deploy tools and analytical software that can be applied and shared to manipulate, transform, and display data and other identified needs.

*Data Governance and Privacy:* In developing the program, the federal government should establish the procedures and data governance structures necessary to protect the sensitivity of data, comply with federal regulations and statutes, and respect existing consent agreements with the private sector and other non-federal entities. The federal government should take steps to make preexisting and all future consent agreements compliant with inclusion into the environment and bring preexisting agreements and programs into compliance with the program.

*Public-Private Partnership:* The environment should be designed with the goal of including the participation of the private sector and information sharing and analysis organizations/centers, both to feed into and to benefit from the data and analytical insight the environment would provide. Initially, elements of systemically important critical infrastructure, as part of their designation, will be encouraged to share cyber threat indicators, malware forensics, and data from network sensor programs.

### *Enabling Recommendations*

#### **5.2.1 Expand and Standardize Voluntary Threat Detection Programs**

Current voluntary network monitoring and threat detection programs<sup>294</sup> are essential in advancing a better understanding of threats affecting U.S. critical infrastructure. These voluntary programs, through which the U.S. government provides sensors or funding to monitor private-sector networks, can enable the rapid detection and identification of cyber threats—whether they are isolated incidents or part of a larger, coordinated campaign. While programs like DHS’s Enhanced Cybersecurity Services Program and the Department of Energy’s Cyber Risk Information Sharing Program show great promise, their usefulness has been hindered by a limited scale of deployment and insufficient coverage. In addition, coverage and deployment have not been centrally planned or coordinated to reflect strategic assessment of risk and need. Properly implemented and deployed at sufficient scale, these programs could form the foundation of a virtual “early warning network” in cyberspace, providing a vital missing piece in U.S. government and private-sector situational awareness.

To achieve this goal, the U.S. government should take steps, through the Joint Collaborative Environment’s interagency council, to expand and more centrally fund, manage, and deploy these programs and ensure their interoperability with broader federal cyber threat-sharing and integration efforts. In addition, Congress should identify programs that should be excluded from or have special handling in this expansion and standardization, such as law enforcement and domestic counterintelligence collection efforts.

#### **5.2.2 Pass a National Cyber Incident Reporting Law**

The government’s cyber incident situational awareness, its ability to detect coordinated cyber campaigns, and its risk identification and assessment efforts rely on comprehensive data. However, there are insufficient