FY 2020 Defense Appropriations Request
Making Critical Infrastructure Cyber Customers of the Intelligence Community: A Win-Win for the Public and Private Sectors

Summary

- Congress funds a critical infrastructure and intelligence community cybersecurity risk mitigation program (the cyber program) at the Office of the Director of National Intelligence (ODNI) to facilitate the voluntary designation of critical infrastructure entities as customers of the intelligence community (IC).

- Policymakers should make cyber threats against critical infrastructure a priority across the IC. A program for routine public-private analytic efforts does not exist.

Background: Deepening Operational Collaboration to Protect Critical Infrastructure

The responsibility to protect U.S. critical infrastructure against malicious cyber activity is shared by the private sector and the federal government. Industry, similar to government, is exposed to unrelenting, often state-sponsored cyberattacks, which are eclipsing the threat of physical terrorist acts. However, unlike government, businesses lack the intelligence collection authorities and capabilities to push back effectively against foreign powers and criminal groups.[1]

This challenging landscape is forcing government and business leaders to rethink cybersecurity, including more assertively protecting the nation's critical functions.[2] Over the past decade, industry's direct experience with cyberattacks, media reporting, and public policy have overwhelmingly made the case for greatly improving operational collaboration between the business community and government, especially the IC.[3]

Funding Request: Making Voluntary Private Entities Intelligence Customers and Supporting IC Analysts

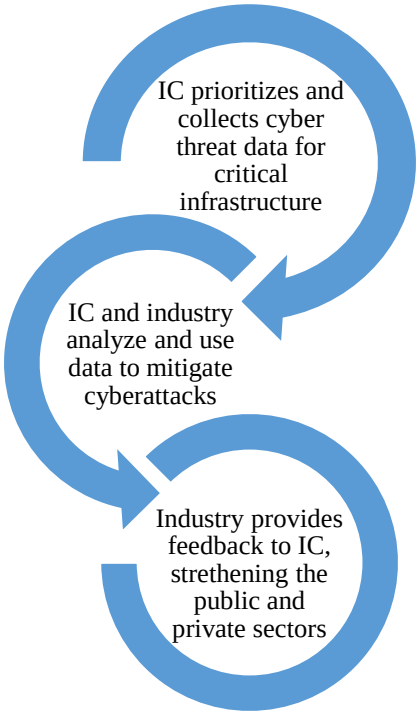
The U.S. Chamber of Commerce believes that the IC should collect and share classified cybersecurity threat data with businesses critical to the economy. To be sure, substantial sharing of cyber threat information exists between agencies and industry. There is, however, a consensus that we need to do much better, particularly against the persistent, malicious activity initiated by nation states or their surrogates and criminal syndicates.[4]

The Chamber urges House and Senate appropriators to fund a cyber program at the ODNI that enables critical infrastructure entities to be *voluntarily identified as customers* of the IC. High-level discussions have been ongoing for years, yet concrete results are difficult to pinpoint. We have downplayed a legislative fix over the last few years, but the lack of tangible outcomes benefiting industry suggests that legislation is necessary.

The cyber program will represent a key step toward a deeper, more structured relationship than the current cyber information-sharing process. To be effective, intelligence should be both informed by and useable by the consumer. This will be nearly impossible absent a regular program of joint analytic collaboration between IC experts—who will likely require additional resources and policy support—and private defenders. Such a program for routine side-by-side analytic efforts does not exist today.

The Chamber is engaging Capitol Hill and the administration on how our organization can help the IC deliver actionable threat information to critical infrastructure actors in a timely way. Such an outcome should be viewed as a win-win for the public and private sectors.

IC Collection for Industry Will Strengthen U.S. Economic and National Security



Language Request

Critical infrastructure and intelligence community cybersecurity risk mitigation program (the cyber program).—The Committee believes that cyber threats against critical infrastructure, particularly attacks by foreign actors, need to be a higher priority for intelligence collection and analysis across the Intelligence Community (IC). Better, more timely intelligence is needed by critical infrastructure owners and operators to detect, prevent, and mitigate unauthorized activity by nation states or their proxies and criminal groups against them. The Committee notes that the IC has unique authorities and capabilities to produce information that can greatly improve the defense of the nation's critical infrastructure. It therefore directs the Office of the Director of National Intelligence (ODNI) to collaborate with critical infrastructure sectors, on a voluntary basis, to create the critical infrastructure and intelligence community cybersecurity risk mitigation program (the cyber program).

The initial mission of the cyber program would be to provide a hub for joint IC/industry intelligence management of collection priorities, analysis, and dissemination. The intelligence analyzed and disseminated under the cyber program should be used by public- and private- sector participants to prioritize risk mitigation activities to protect U.S. critical infrastructure and, by extension, U.S. economic and national security. This partnership program should begin with the establishment of a cadre of analysts dedicated to the energy and financial services sectors. Within available funds, $5,000,000 is recommended for the cyber program. The ODNI is directed to provide a report of the status of the implementation of this section within 90 days of enactment of this Act, and quarterly thereafter, and provide joint recommendations with the participating critical infrastructure sectors on how future collection requirements can be prioritized within 180 days.

(Revised April 26, 2019)

Notes

---

[1] See, for example, Aspen Institute, *An Operational Collaboration Framework for Cybersecurity* (November 2018); Carnegie Endowment for International Peace, *Protecting Financial Institutions Against Cyber Threats: A National Security Issue* (September 2018); and the Council on Foreign Relations, *Sharing Classified Cyber Threat Information With the Private Sector* (May 2018).

[2] On July 31, 2018, in announcing the Department of Homeland Security's (DHS') new National Risk Management Center, Secretary Kirstjen Nielsen described today's disturbing reality in cyberspace: "[C]yber threats collectively now exceed the danger of physical attacks against us. This is a major sea change . . . for our country's security." DHS Secretary Kirstjen M. Nielsen's National Cybersecurity Summit Keynote Speech (July 31, 2018).

[3] The Government Accountability Office (GAO) testified before Congress and said that urgent actions are needed by the federal government and industry to protect cyber critical infrastructure. GAO, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation* (GAO-18-645T), July 25, 2018.

[4] Executive Order 12333, which was released in 1981 and last amended in 2008, says, "Our national intelligence effort should take into account the responsibilities and requirements of … as appropriate, *private sector entities,* when undertaking the collection and dissemination of information and intelligence to protect the United States" [italics added].