THE
NATIONAL LAW REVIEW

New Cybersecurity Report Asks the Private Sector to Join Forces with the Government

McDermott Will & Emery

Article By
Michael G. Morgan
McDermott Will & Emery
Of Digital Interest

- Communications, Media & Internet
- All Federal

Wednesday, September 13, 2017

The National Infrastructure Advisory Council (NIAC) recently published a report that identifies cyber threats and urges private companies and executives to join forces with the government to better address those threats. *See* The President's National Infrastructure Advisory Council, *Securing Cyber Assets, Addressing Urgent Cyber Threats to Critical Infrastructure* (Aug. 15, 2017) (NIAC Report). Among other things, the report cites the lack of information sharing and coordination between private parties and various governmental bodies as a primary reason why the nation "remain[s] unable to move actionable information to the right people at the speed required by cyber threats." NIAC Report, at 5. According to NIAC, "it is imperative that Federal and private roles in defending these systems are aligned and mutually supportive." NIAC Report, at 5.

In short, the government is asking for private sector help in its fight against cyber attacks. NIAC's proposals include "public-private and company-to-company information sharing of cyber threats at network speed." NIAC Report, at 8. NIAC refers to risks associated with sharing "real-time system data with the Federal Government" including unspecified "significant business risks and liability" issues. NIAC Report, at 8. NIAC does not propose any specific way to alleviate those risks, but states that a pilot program should be used to "work through legal and liability barriers." NIAC Report, at 8. NIAC also makes some general references to incentives that could be provided to private parties for their participation. While NIAC does

provide a number of useful suggestions, many of the issues that are most important to private sector participants are not described in detail. First, NIAC has not provided any specifics about the incentives the government would be willing to offer. Second, though NIAC has identified unspecified risks associated with sharing information with the government it has not provided any guidance about how to limit those risks.

The President Ordered a Review of the Nation's Cybersecurity System

On May 11, 2017, President Trump issued Executive Order 13800 titled *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. The president noted that "the executive branch has for too long accepted antiquated and difficult-to-defend IT." Exec. Order No. 13800, ¶ 1(b)(ii). The Executive Order also states that "known but unmitigated vulnerabilities are among the highest cybersecurity risks faced by executive departments and agencies" and the "known vulnerabilities include using operating systems or hardware beyond the vendor's support lifecycle, declining to implement a vendor's security patch, or failing to execute security-specific configuration guidance." Exec. Order No. 13800, ¶ 1(b)(iv).

NIAC was established in 2001 to advise the president on practical strategies for industry and government to reduce complex risks to the designated critical infrastructure sectors. In support of Executive Order No. 13800, the National Security Council asked NIAC to identify cybersecurity issues and examine "how Federal authorities and capabilities can best be applied to support cybersecurity of high-risk assets." NIAC Report, at 2. On August 15, 2017, NIAC issued its report.

NIAC's Report Asks Private Parties to Coordinate with the Government to Defend against Cyber Attacks

NIAC's Report contains a number of suggestions and requests for participation from private parties. The Report remarks that NIAC "believes the U.S. government and private sector collectively have the tremendous cyber capabilities and resources needed to defend critical private systems from aggressive cyber attacks—provided they are properly organized, harnessed, and focused. Today, we're falling short." NIAC Report, at 3, 5. Most of NIAC's suggestions relate to information sharing and the need for "the Federal Government to apply its collective authorities and capabilities in concert with the private sector." NIAC Report, at 5.

NIAC recommends a "private-sector-led pilot of machine-to-machine information sharing technologies" in order to "test public-private and company-to-company information sharing of cyber threats at network speed." NIAC Report, at 3. One key task that the NIAC recommends is to "work through legal and liability barriers that hamper or limit company-to-company and government-to-company sharing today." NIAC Report, at 8. The report notes that this sort of information sharing would require "significant trust regarding how information will be protected, shared, and used." NIAC Report, at 8. NIAC also notes that "leaked data creates significant business risks and liability protections are not court-tested." NIAC Report, at 8. NIAC makes various references to "business risks and liability protections," "legal and liability barriers that hamper or limit company-to-company and government-to-

company sharing today" and "significant legal, liability, technology, trust, and cost challenges." NIAC Report, at 8, 15. However, NIAC does not provide any information as to what those business risks and liability barriers actually are and what private sector participants can do to alleviate those concerns.

It further recommends a public-private "task force of experts in government and the electricity, finance, and communications industries" and an "optimum cybersecurity governance approach to direct and coordinate the cyber defense of the nation." NIAC Report, at 4. NIAC states that the government "must champion cybersecurity with the private sector" and "direct an operational team of cross-agency, public-private staff to triage and make headway on the biggest needs." NIAC Report, at 17. NIAC also suggests detailed testing of the government's reactions to cyber incidents and to "invite executives and representatives from the Financial Services and Communications sectors to participate in exercise planning, ownership, and execution." NIAC Report, at 18. NIAC also recommends expedited declassification of cyber threat information to be shared with owners and operators of critical infrastructure. NIAC Report, at 4. It states that the present "inability to rapidly declassify and share the less-sensitive elements of a potential threat, like threat indicators or vulnerabilities, leaves private companies in the dark for too long." NIAC Report, at 14. To help with the declassification, NIAC also wants to "engage and embed cleared private sector representatives from the most critical infrastructure asserts in government intelligence and information sharing centers to help inform and prioritize information declassification." NIAC Report, at 14.

Incentives for Upgrading Cyber Infrastructure and Attempting to Increase the Cybersecurity Work Force

NIAC also references unspecified incentives that should be given to those private sector parties who strengthen cybersecurity infrastructures. It suggests "limited time, outcome-based market incentives that encourage owners and operators to upgrade cyber infrastructure, invest in state-of-the-art technologies, and meet industry standards or best practices." NIAC Report, at 12. NIAC also suggests that organizations should be incentivized to adopt the NIST Cybersecurity Framework (which was itself created "through collaboration between government and the private sector"). *See* National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0* (Feb. 12, 2014). A draft version of a revised framework was released on January 10, 2017. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, Draft Version 1.1* (Jan. 10, 2017); NIAC Report, at 12. However, there are no specifics as to what incentives will be given or how "out-come based market incentives" could or would be determined. NIAC Report, at 12.

NIAC notes a shortfall of qualified cybersecurity professionals which it estimates will result in 1.8 million unfilled positions by 2011. NIAC Report, at 11. It suggests scholarships and sponsorship clearances for college-age prospective cyber professionals. NIAC Report, at 11. In this area too, NIAC suggests private sector participation stating that "federal cyber experts have a limited understanding of unique private sector systems, which limits their ability to provide technical assistance." NIAC Report, at 11. NIAC also recommends identifying and employing "best-in-class Scanning Tools and Assessment Practices" and streamlining and

significantly expediting the Security Clearance Processes and declassification processes to ensure that key persons can “access secure facilities within one hour of a major threat or incident.” NIAC Report, at 10, 13.

Conclusion

NIAC states that the “time to act is now” and “as a Nation, we need to move past simply studying our cybersecurity challenges and begin taking meaningful steps to improve our cybersecurity to prevent a major debilitating attack.” NIAC Report, at 21. NIAC has doled out a number of tasks to various government agencies and requested significant assistance from private parties. However, the government has yet to give guidance to private sector participants related to the incentives it will offer and how to limit the unspecified liability concerns referenced in the NIAC Report. The private sector will need to continue waiting for guidance on these critical issues, each of which contributes to the lack of information sharing and increased cybersecurity infrastructure that NIAC hopes to address.

Source URL: https://www.natlawreview.com/article/new-cybersecurity-report-asks-private-sector-to-join-forces-government