INTELLIGENCE INSIGHTS

EXPERT INSIGHTS ON NATIONAL SECURITY DEVELOPMENTS

MAY 2021

Views on DoD Cyber Threat Hunting on Defense Industrial Base Networks

PRESENTED BY INSA'S CYBER COUNCIL

CYBER COUNCIL

A joint statement released on February 3, 2021 by House Armed Services Committee Chairman Adam Smith (D-WA) and Congressman James Langevin (D-RI) said the "…Fiscal Year 2021 National Defense Authorization Act (NDAA) has widely been touted as the most significant piece of cybersecurity legislation ever to pass Congress."

The NDAA has more than 50 individual sections and provisions to strengthen the governance of federal cybersecurity, protect US critical infrastructure, and advance cyber threat information sharing between the public and private sectors. The common goal of these provisions is to strengthen the cyber resiliency of the United States against an ever-increasing level of activity by criminals, hackers, and nation-state adversaries.

One provision in particular requires extensive dialogue between government and industry to ensure that the intent of Congress can be implemented effectively. Section 1739 of the legislation calls for the Secretary of Defense to assess the feasibility and suitability of "a defense industrial base cybersecurity threat hunting program to actively identify cybersecurity threats and vulnerabilities within the defense industrial base." The legislation directs that the assessment be completed around September 2021 (270 days from the NDAA enactment) and, if the Secretary determines a program is feasible and suitable, that it be implemented by roughly March 2022.

The statute directs that the Secretary "consult with and solicit recommendations from representative industry stakeholders across the defense industrial base" regarding a proposed program and the costs of stakeholder compliance. Towards this end, INSA provides these recommendations on the proposed defense industrial base (DIB) cybersecurity threat hunting program as envisioned by Section 1739.

DIB companies are committed to protecting their privately-owned networks from adversarial attacks for a range of reasons, including:

- Reputational damage caused by a significant cyber incident would negatively impact a company's business.
- Loss of intellectual property could lead to counterfeit or competing products which would harm a company's future revenue streams.
- Intrusions of ransomware or destructive malware could impair a company's operations and cause extensive financial and reputational harm.
- Implantation of malware or the modification of an existing code or blueprint base for national security products could negatively impact its performance, potentially affecting military operations.
- Companies have an interest in protecting private information regarding their employees, partners, and clients that resides on these networks.

Paragraph (b) of Section 1739 specifies that the Secretary of Defense's assessment evaluate seven specified elements (listed below). INSA provides the following recommendations regarding each element for DoD to consider as it begins its collaboration with industry:

1 **Evaluate existing DIB cybersecurity threat hunting policies and programs, including the threat hunting elements at each level of the Cybersecurity Maturity Model Certification (CMMC).**

RECOMMENDATION: Large DIB companies will likely be certified at the highest CMMC level and are likely already performing some type of threat hunting. The challenge lies with the small-to-mid-size companies that may be investing heavily to develop a marketable product and/or market position while endeavoring to meet CMMC requirements at an affordable cost. A cyber threat hunting program requirement will place increased financial burdens on these companies. These small-to-mid-size companies may require technical and financial assistance to remain part of a viable national defense supply chain, and must be assessed as to the level of risk they might represent to the supply chain at their current CMMC capability. Technical assistance could come in the form of trusted third party vendors while financial assistance could be a function of US government contracting by making the cost an "allowable cost" under DoD acquisition regulations.

2 **Evaluate the suitability of a continuous cyber threat hunting program including the consideration of: (a) collection and analysis of metadata on DIB network activity, (b) rapid investigation and remediation of possible intrusions, (c) requirements for mitigating any vulnerabilities, and (d) mechanisms for DoD to share cyber threat information with the DIB.**

RECOMMENDATION: Companies should compile and assess the metadata on their own networks, which will help them determine whether threats exist. DIB companies should provide DoD their

threat analyses, which would discuss threat indicators such as those contained in metadata. However, because such metadata could include personally identifying information (PII) that requires special protection (e.g., legal or medical data), as well as proprietary intellectual property, DoD should not require DIB companies to provide the actual metadata. Significantly, a requirement to provide PII may be inconsistent with some U.S. laws (e.g., the California Consumer Privacy Act) and non-U.S. laws (e.g., the European Union's General Data Protection Regulation) and thus require DIB companies to reconfigure their networks and business processes to ensure compliance.

Under element 2(d), the focus should be on how DoD can better share information to assist companies in their threat hunting activities. Potentially, some of the most valuable DoD information would be USG intelligence on potentially upcoming and/or developing cyber threats using real intelligence and predictive analytics.

3 **Evaluate recommendations for DIB primes' and subcontractors' participation in the cybersecurity threat hunting program relating to: (a) incentives, (b) mandating minimum levels of participation, (c) procurement prohibitions, (d) waiver authority and criteria and (e) a tiered program which considers (i) cybersecurity maturity of DIB entities, (ii) the roles of such entities, (iii) whether these entities possess classified or controlled unclassified information and (iv) the covered information to which each entity has access as a result of DoD contracts.**

RECOMMENDATION: This element directs the Secretary to explore whether "carrots" or "sticks" (incentives or procurement prohibitions) are more likely to encourage industry to comply. Because companies universally support advancements in cybersecurity, the Secretary's assessment should focus principally on the incentives, assistance, and potential waivers that may be needed to enable individual companies—particularly small firms with limited resources—to participate in a threat hunting program.

4 **Evaluate whether threat hunting programs should be conducted by: (a) qualified contractors, (b) accredited third-party vendors, (c) US Cyber Command or another DoD component, (d) deployment of DoD sensors on DIB networks, or (e) a combination of the above.**

RECOMMENDATION: Given the complex legal and intellectual property issues associated with a company's data, a company should perform all threat hunting activity on its network itself unless it voluntarily and expressly consents to assistance from DoD or a third-party. A company should not be required to permit an outside party—either a vendor or a government agency—to operate or place sensors on its network. To institute such a requirement, DoD would need clear legislative authority which is not contained in Section 1739.

DoD should evaluate and ultimately employ existing mature and proven commercial technologies that are non-intrusive but effective and scalable. Many DIB primes already leverage continuous cyber threat and risk monitoring and alerting services, using publicly available data sets and AI-based security analytics, that are employed to varying levels across all sectors today. Using these commercial technologies, DIB small and medium-sized businesses that are not cyber sophisticated and do not have the expertise nor the resources to purchase high-end cybersecurity services could have their threats monitored and risks mitigated in a non-intrusive but effective way; but of course, that comes at a cost which small business may not be able to absorb.

5 Evaluate the resources, governance structures or changes in regulation or law to execute the program.

RECOMMENDATION: Companies participating in a threat hunting program should be provided liability protections to insulate them from lawsuits related to disclosure of third-party data; such protection, however, would likely require further legislative action.

Small companies would likely lack the resources and expertise needed to participate in such a program, which could deter them from pursuing DoD contracts and remaining viable members of the DoD supply chain. DoD should provide resources to mitigate the costs to small DIB companies or specify related expenses as "allowable costs" under DoD contracts.

6 Evaluate the timeline for establishing the program within two years of enactment (by January 2023).

RECOMMENDATION: Using the CMMC as a model, a cyber threat hunting program should be rolled out slowly to establish the program's value and to assess first-, second-, and third-order effects on the DIB supply chain. Some of these consequences could include companies refusing to allow USG sensors on their networks, what to do in cases of industry data loss as a result of DoD threat hunting operations, what happens if threat hunting causes the company's system to crash and more. Additionally, information discovered through cyber threat hunting could trigger compliance actions—such as incident reporting, threat mitigation measures, and referrals to counterintelligence or law enforcement authorities—from a broad range of DoD entities involved in the contracting process. Such actions may create legal liabilities or obstacles to contract execution that create business risks for the affected company. In an attempt to identify and mitigate these concerns, DoD could conduct several tabletop exercises, then begin a pilot program, then expand a program to a few contracts while assessing its value and identifying potentially adverse impacts on the viability of DIB companies.

7 Identify any barriers that would prevent the establishment of the program.

RECOMMENDATION: Any approach that would allow DoD to have unfettered access to DIB networks to conduct cyber threat hunting, when there is no indication of an internal threat nor a predicate for law enforcement investigation, would require additional legislative authorities. To mitigate legal, liability, and privacy barriers, any cyber threat hunting program should be voluntary, company-managed and -controlled, and share tailored categories of information; even then, companies would seek liability protection, which would require further statutory authority.

SEC. 1739. ASSESSMENT ON DEFENSE INDUSTRIAL BASE CYBERSECURITY THREAT HUNTING PROGRAM.

(a) ASSESSMENT REQUIRED.—Not later than 270 days after the date of the enactment of this Act, the Secretary of Defense shall complete an assessment of the feasibility, suitability, definition of, and resourcing required to establish a defense industrial base cybersecurity threat hunting program to actively identify cybersecurity threats and vulnerabilities within the defense industrial base.

(b) ELEMENTS.—The assessment required under section (a) shall include evaluation of the following:

(1) Existing defense industrial base cybersecurity threat hunting policies and programs, including the threat hunting elements at each level of the compliance-based Cybersecurity Maturity Model Certification program of the Department of Defense, including requirements germane to continuous monitoring, discovery, and investigation of anomalous activity indicative of a cybersecurity incident.

(2) The suitability of a continuous cybersecurity threat hunting program, as a supplement to the cyber hygiene requirements of the Cybersecurity Maturity Model Certification, including consideration of the following:

(A) Collection and analysis of metadata on network activity to detect possible intrusions.

(B) Rapid investigation and remediation of possible intrusions.

(C) Requirements for mitigating any vulnerabilities identified pursuant to the cybersecurity threat hunting program.

(D) Mechanisms for the Department of Defense to share with entities in the defense industrial base malicious code, indicators of compromise, and insights on the evolving threat landscape.

(3) Recommendations with respect to cybersecurity threat hunting program participation of prime contractors and subcontractors, including relating to the following:

(A) Incentives for defense industrial base entities to share with the Department of Defense threat and vulnerability information collected pursuant to threat monitoring and hunting activities.

(B) Mandating minimum levels of program participation for any defense industrial base entity.

(C) Procurement prohibitions on any defense industrial base entity that is not in compliance with the requirements of the cybersecurity threat hunting program.

(D) Waiver authority and criteria.

(E) Consideration of a tiered cybersecurity threat hunting program that takes into account the following:

(i) The cybersecurity maturity of defense industrial base entities.

(ii) The roles of such entities.

(iii) Whether each such entity possesses classified information or controlled unclassified information and covered defense networks.

(iv) The covered defense information to which each such entity has access as a result of contracts with the Department of Defense.

(4) Whether the continuous cybersecurity threat-hunting program described in paragraph (2) should be conducted by—

(A) qualified prime contractors or subcontractors;

(B) accredited third-party cybersecurity vendors;

(C) with contractor consent—

(i) United States Cyber Command; or

(ii) a component of the Department of Defense other than United States Cyber Command;

(D) the deployment of network sensing technologies capable of identifying and filtering malicious network traffic; or

(E) a combination of the entities specified in subparagraphs (A) through (D).

(5) The resources necessary, governance structures or changes in regulation or law needed, and responsibility for execution of a defense industrial base cybersecurity threat hunting program, as well as any other considerations determined relevant by the Secretary.

(6) A timelime for establishing the defense industrial base cybersecurity threat hunting program not later than two years after the date of the enactment of this Act.

(7) Identification of any barriers that would prevent such establishment.

(c) CONSULTATION.—In conducting the assessment required under subsection (a), the Secretary of Defense shall consult with and solicit recommendations from representative industry stakeholders across the defense industrial base regarding the elements described in subsection (b) and potential stakeholder costs of compliance.

(d) DETERMINATION AND BRIEFING.—Upon completion of the assessment required under subsection (a), the Secretary of Defense shall make a determination regarding the establishment of a defense industrial base cybersecurity threat hunting program and provide a briefing to the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives on—

(1) the findings of the Secretary with respect to such assessment and such determination; and

(2) such implementation plans as the Secretary may have arising from such findings.

(e) IMPLEMENTATION.—If the Secretary of Defense makes a positive determination pursuant to subsection (d) of the feasibility and suitability of establishing an industrial base threat cybersecurity threat hunting program, the Secretary shall establish such program. Not later than 180 days after a positive determination, the Secretary of Defense shall promulgate such rules and regulations as are necessary to establish the defense industrial base cybersecurity threat hunting program under this section.

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

ACKNOWLEDGEMENTS

INSA expresses its appreciation to the INSA members and staff who contributed their time, expertise, and resources to this piece.

MEMBERS

Jim Keffer, *Lockheed Martin; Cyber Council Chair*

Nancy Landreville, *University of Maryland Global Campus*

Brian O'Callaghan, *Digital Global Connectors*

Steve Shirley, *National Defense ISAC*

Moon Yousif Sulfab, *Virginia Tech*

Christian Vickland, *Deloitte*

Samuel S. Visner, *MITRE*

INSA STAFF

John Doyon, *Executive Vice President*

Larry Hanauer, *Vice President for Policy*

Peggy O'Connor, *Director of Communications and Policy*

Caroline Henry, *Communications and Marketing Assistant*

ABOUT INSA

The Intelligence and National Security Alliance (INSA) is a nonpartisan, nonprofit forum for advancing intelligence and national security priorities through public-private partnerships. INSA's government and private sector members collaborate to make government more effective and efficient through the application of industry expertise and commercial best practices. INSA's 160+ member organizations are leaders in intelligence collection and analysis, data analytics, management consulting, technology development, cybersecurity, homeland security, and national security law, and its 4,000 individual and associate members include leaders, senior executives, and intelligence experts in government, industry, and academia.

ABOUT INSA'S CYBER COUNCIL

INSA's Cyber Council seeks to fuse knowledge from industry, government, and academic experts in order to provide authoritative and influential insights regarding the national security challenges present in the cyber domain. The Council works to promote a greater understanding of cyber threats, challenges, and opportunities that can be addressed effectively through public-private collaboration.