CISA CYBERSECURITY ADVISORY COMMITTEE

REPORT TO THE CISA DIRECTOR

Optimizing CISA's Cyber Operational Collaboration Platform

Date: June 5, 2024

Introduction:

The Cybersecurity and Infrastructure Security Agency (CISA) tasked the Cybersecurity Advisory Committee (CSAC) with developing strategic recommendations to support the continued maturation, investment, and focus of CISA's Joint Cyber Defense Collaborative (JCDC). The CSAC established the Optimizing CISA's Cyber Operational Collaboration Platform subcommittee (OCP) to advance this tasking. JCDC's public-private cybersecurity collaboration leverages new authorities granted by Congress in the National Defense Authorization Act (NDAA) of 2021 to develop— for public and private sector entities— plans for cyber defense operations. This includes the development of a set of coordinated actions to protect, detect, respond to, and recover from cybersecurity risks or limit against coordinated cyber operations that pose a potential risk to national interests.

Specifically, the Committee was tasked with providing recommendations on an optimal state for operational cyber defense collaboration, incorporating all aspects of JCDC's mission. Specific focus areas include collaboration, planning, and product development.

CISA's cyber defense mission is dependent upon effective operational collaboration between government and the private sector, which it enables in significant part through JCDC. Over the past three years, JCDC has achieved significant milestones, but CISA knows that the collaboration model remains in an early stage. CSAC is asked to consider and provide recommendations on an optimal state for operational cyber defense collaboration, incorporating all aspects of JCDC's mission, in the interest of informing continued maturation, investment, and focus. Specific questions include:

<u>Collaboration</u>

1) How do industry partners assess value from participating in CISA's operational collaboration efforts?
2) How can CISA most effectively identify and support industry partners to participate in operational collaboration efforts?
3) What are potential constraints that may limit the effectiveness or breadth of operational collaboration between CISA and industry partners?
4) What are steps that CISA can take to address constraints potentially limiting operational collaboration, including technology, process, or personnel improvements?

<u>Planning</u>

1) How do industry partners assess value from participating in CISA's joint cyber planning efforts?
2) How should CISA select or develop issues for cyber defense planning efforts that create the most impact for stakeholders?

<u>Product Development</u>

1) What is the value proposition for CISA's cybersecurity product to stakeholders?
2) How can CISA most effectively incorporate industry and partner feedback in cyber defense products?

Findings:

The outlined recommendations are guided by the eight scoping questions in three subject areas provided to the Committee by CISA. The recommendations are informed by subcommittee meetings which assessed the current state of JCDC from the public sector, trade groups, industry leaders, and private sector experts.

CISA established JCDC on August 5, 2021. As of May 6, 2024, there are 321 total partner organizations with direct representation from 12 critical infrastructure sectors (Chemical, Commercial Facilities, Communications, Critical Manufacturing, Defense Industrial Base, Energy, Financial Services, Food and Agriculture, Healthcare and Public Health, Information Technology, Transportation Systems, and Waste and Wastewater). JCDC partners provide services to and derive insights from all critical infrastructure sectors.

Throughout all the subcommittee's briefings, the subcommittee consistently heard about the value that JCDC has brought to national security. Specifically, briefers pointed to the collaboration, operationally-focused discussion, and near-real-time bi-directional flow of intelligence around the U.S.'s response to the Russia-Ukraine conflict as a strong example of a successful model to build on. The subcommittee also heard feedback on some areas for improvement that have been identified during the nearly three years of activity. These opportunities to strengthen JCDC inform the following recommendations.

Recommendations:

- **Continue to amplify JCDC's focus on operational cyber defense.** Today, JCDC has representation from the cybersecurity community at both technical/operational and public policy levels. On a technical/operational level, JCDC has delivered substantial value in key international events like the Russia-Ukraine conflict and the Log4j vulnerability and should build on these successes.
    - JCDC should continue and deepen its focus on operational collaboration and serve as a resource for those organizations involved in public policy.
        - **Ideal End State:** If this is successful, JCDC's day-to-day activities will center around operational collaboration, active incidents, or potential incidents. While JCDC and its members may be consulted on policy-centric questions, daily activities will not revolve around policy.

- **Clarify key operational components of JCDC– specifically, criteria for membership and participation in physical collaboration spaces.** Clarity and transparency around membership requirements and joining process would help to deepen JCDC's impact and value. JCDC should include elements of the federal agencies that engage in collaboration with the private sector to foster deeper coordination within the federal government. Further, there would be benefit in formalizing the structure and on-going participation requirements for physical collaboration spaces. By bringing together the right entities for in-person collaboration, JCDC can deepen trust amongst participants and streamline the bi-directional sharing of actionable intelligence that is key for operational response.
    - JCDC, in conjunction with key stakeholders, needs to develop clear criteria for participation in information sharing activities within 60 days.
        - **Ideal End State:** If this is successful, JCDC's purpose, what it does, and the criteria for membership will be clear to not only current participants in JCDC– but also to others interested in potentially becoming a member. Further, the criteria to remain a member and continue to participate in the various information sharing mechanisms within JCDC will also be clarified.

- **Leverage the convening power of JCDC to build out Coordinating Structures such as a proactive 'Smart Rolodex' of public and private partners.** A smart rolodex is a roster of the public and private sector members and their core competencies designed to make identifying potential partners simpler. CISA should connect these partners

both proactively and reactively to improve the nation's collective defense capabilities. JCDC is uniquely positioned to deepen these key connections.

- To develop and test these Coordinating Structures, JCDC should identify an issue to exercise on a periodic basis not less than semi-annually. Following the exercise, JCDC can mitigate risks and identify areas of improvement.
  - **Ideal End State:** If this is successful, JCDC will have a clear process for continuing to identify the appropriate partners for given situations and requests. Further, JCDC will have an enhanced ability to respond to active issues while proactively preparing for future issues.

Appendix:

The following OCP subcommittee members participated in the study and recommendations documented in this report.

Ron Green, OCP Subcommittee Chair, Mastercard
Brett DeWitt. Mastercard
Will Garrity, Mastercard
Brian Gragnolati, Atlantic Health System
Niloofar Razi Howe, Tenable
Chris Inglis, Former Office of the National Cyber Director
Jim Langevin, Former U.S. House of Representatives
Meraz Nasir, Atlantic Health System
Alex Tosheff, Former VMware
Angela Weinman, Former VMware