


October 10, 2024

MEMORANDUM FOR THE CYBERSECURITY ADVISORY COMMITTEE MEMBERS

FROM: Jen Easterly 
Director
Cybersecurity and Infrastructure Security Agency (CISA)

SUBJECT: **Formal Response to Recommendations Provided on June 5, 2024**

The Cybersecurity Advisory Committee (CSAC) was established in June 2021 to advise, consult with, report to, and make recommendations to the Cybersecurity and Infrastructure Security Agency (CISA) on the development, refinement and implementation of policies, programs, planning, and training pertaining to CISA's cybersecurity mission. Since that time, the CSAC has provided strategic recommendations, leveraging their members' significant subject-matter expertise, into CISA's cybersecurity mission.

CISA values the hard work of the CSAC that led to a set of actionable recommendations to improve on CISA's execution of its cybersecurity mission. The expert advice and key insights that the CSAC offers will enhance the work of CISA and keep us well-positioned to help address threats in a rapidly changing cybersecurity landscape.

I have worked closely with my leadership team to determine the feasibility of each recommendation and to ensure that we remain within the legal parameters of CISA's operating authorities and resources. Our response to each subcommittee is as follows:

Response to the Optimizing CISA's Cyber Operational Collaboration Platform Subcommittee

Recommendations 1 – 3

Addressing Recommendation #1: The Joint Cyber Defense Collaborative (JCDC) has made significant progress that aligns with the Subcommittee's recommendation to "continue and deepen its focus on operational collaboration and serve as a resource for those organizations involved in public policy." In recent months, JCDC has implemented measures to ensure greater awareness and inclusion of JCDC members into day-to-day operational collaboration activities. JCDC has established new channels to communicate priority incidents and events requiring focused public-private information sharing and enrichment, as well as publishing a monthly partner dashboard to communicate the status and developments of JCDC cyber defense initiatives, current and future publications, and threat information sharing activities. These outreach efforts are intended to transparently reflect JCDC's operational focus in the moment as well as increase overall engagement of JCDC members in priority near-and medium-term efforts to protect against threats to the nation's critical infrastructure. JCDC is also planning several analytical exchanges around priority efforts (e.g., cloud security and Operational Technology (OT) security) that will provide expanded opportunities for partners to contribute and engage.

Addressing Recommendation #2: JCDC is currently studying its existing partnership structure to include an evaluation of its member selection criteria, value proposition, and engagement across its diverse member-base. Outcomes of the study will include development/evolution of membership communities, organized by common capabilities or threat visibility (i.e., via threat intelligence/security providers), collaborative initiatives (i.e., artificial intelligence (AI), OT/industrial control systems (ICS), etc.), or critical infrastructure protection role (i.e., asset management/portfolio companies, cyber insurers, etc.). These sub-communities would be aligned to specific threat intelligence enrichment activities and/or collaborative initiatives based on their role, capabilities, or influence in advancing security outcomes for the broader cyber defense community.

Addressing Recommendation #3: JCDC is conducting ongoing research and technical development to populate its JCDC member database that includes information on member capabilities. As noted in the recommendation, this information is intended to be used to identify and align partners with threat information sharing engagement and cyber defense initiative opportunities.

Aside from refining its onboarding questionnaire of new members and conducting research to enrich information held about current members, JCDC intends to dedicate resources to maintaining a business intelligence capability within its partner management function and is engaged in discussions to migrate its member database to CISA's stakeholder relationship management (SRM) platform. When completed, the migration will enable shared situational awareness of member engagement with other stakeholder-facing missions within CISA (e.g., Stakeholder Engagement Division, Integrated Operations Division's regional staff).

The effectiveness of these membership convening, connection, and coordination structures will be reviewed through a series of exercises JCDC will facilitate and/or participate in, across a variety of operational communities.

Again, I thank the CSAC and its members for their thoughtful recommendations. Please feel free to contact me if you have any questions. We look forward to continued partnership with the CSAC.

List of Recommendations and Responses

	Recommendation	Response	Non-Concur Justification	ECD
1	<p>Recommendation: Continue to amplify CISA’s Joint Cyber Defense Collaborative (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.</p> <ul style="list-style-type: none"> • JCDC should continue and deepen its focus on operational collaboration and serve as a resource for those organizations involved in public policy. <ul style="list-style-type: none"> ○ 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. 	Concur		Steps to communicate operational focus have been completed. The overarching focus on operations is ongoing.
2	<p>Recommendation: 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</p>	Concur		TBD (will complete within 60 days of DIR’s acceptance of this recommendation)

	<p>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.</p> <ul style="list-style-type: none"> • JCDC, in conjunction with key stakeholders, needs to develop clear criteria for participation in information sharing activities within 60 days. <ul style="list-style-type: none"> ○ 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. 			
3	<p>Recommendation: 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.</p> <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> ○ 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 	Concur		The next exercise where JCDC can test its coordination structures will be JCDC.ai in late September, however the goal requires ongoing exercises semi-annually.

	will have an enhanced ability to respond to active issues while proactively preparing for future issues.			
--	----------------------------------------------------------------------------------------------------------	--	--	--