Written Testimony of

John S. Miller
Senior Vice President of Policy and General Counsel
Information Technology Industry Council (ITI)

Before the

Committee on Homeland Security and Government Affairs

United States Senate

The Cyber Safety Review Board:
Expectations, Outcomes and Enduring Questions

January 17, 2024

Written Testimony of
John S. Miller
Senior Vice President of Policy and General Counsel
The Information Technology Industry Council (ITI)

Before the

United State Senate
Homeland Security and Governmental Affairs Committee

"The Cyber Safety Review Board: Expectations, Outcomes, and Enduring Questions"

January 17, 2024

Chairman Peters, Ranking Member Paul, and Distinguished Members of the Homeland Security and Governmental Affairs Committee, thank you for the opportunity to testify today. My name is John Miller, Senior Vice President of Policy and General Counsel at the Information Technology Industry Council (ITI).[1] I lead ITI's Trust, Data, and Technology team, including our work on cybersecurity, privacy, and artificial intelligence policy in the U.S. and globally, and I have deep experience working on public-private cyber, supply chain, and national security initiatives with the Cybersecurity and Infrastructure Security Agency (CISA) and other federal agencies in the United States. I currently serve as Co-chair of the CISA-sponsored Information and Communications Technology Supply Chain Risk Management Task Force (ICT SCRM Task Force) and on the Executive Committee of the Information Technology Sector Coordinating Council (ITSCC), the principal IT sector partner to CISA on critical infrastructure protection and cybersecurity policy (after previously serving consecutive terms as ITSCC Chair). I have also previously served as a principal IT sector representative to the Enduring Security Framework, and on multiple National Security and Telecommunications Advisory Committee (NSTAC) subcommittees, most recently as an appointee to the Subcommittee on Addressing the Misuse of Domestic Infrastructure by Foreign Malicious Actors. I am honored to testify this morning on the Cyber Safety Review Board ("CSRB" or "Board"), including its membership and governance,

[1] The Information Technology Industry Council (ITI) is the premier global advocate for technology, representing the world's most innovative companies. Founded in 1916, ITI is an international trade association with a team of professionals on four continents. We promote public policies and industry standards that advance competition and innovation worldwide. Our diverse membership and expert staff provide policymakers the broadest perspective and thought leadership from technology, hardware, software, services, manufacturing, and related industries. Visit https://www.itic.org/ to learn more.

and how this body established in Executive Order 14028 on *Improving the Nation's Cybersecurity* (EO 14028) can add value to the cybersecurity ecosystem.[2]

ITI represents eighty of the world's leading information and communications technology (ICT) companies.[3] We promote innovation worldwide, serving as the ICT industry's premier advocate and thought leader in the United States and around the globe. ITI's membership comprises leading innovative companies from all corners of the technology sector, including hardware, software, digital services, semiconductor, network equipment, cloud, cybersecurity and other internet and technology-enabled companies that rely on ICT to evolve their businesses – and we accordingly represent a breadth of perspectives reflective of the diversity of our sector. Our companies service and support the global ICT marketplace via complex supply chains in which products are developed, made, and assembled in multiple countries, and service customers across all levels of government and the full range of global industry sectors, including financial services, healthcare, and energy. We thus acutely understand the importance of cybersecurity as not only a global priority for governments, companies, and customers alike, but as critical to our collective security. Our members take seriously the U.S. government's national security imperative to strengthen the security and resilience of the digital ecosystem and have devoted significant resources, including expertise, initiative, and investment in cybersecurity as well as supply chain risk management efforts to create a more secure and resilient Internet ecosystem.

Our members also understand we cannot tackle current and future cybersecurity challenges on our own. We recognize public-private partnerships and other multi-stakeholder approaches are essential to addressing our shared security challenges and have thus prioritized working as a trusted partner with the U.S. government and other governments around the world to help develop cybersecurity as well as supply chain security policy solutions, including developing, supporting and helping to lead public-private mechanisms to advance our shared security priorities. We believe the U.S. government and industry must work together, along with global partners and allies, to build a mutually beneficial cybersecurity community founded on the trusted exchange of information. Our members have for years prioritized building information sharing relationships with relevant U.S. Government stakeholders as well as the global cybersecurity community and have supported the development of policies and standards to promote the voluntary sharing of cybersecurity threat information, including to support the *Cybersecurity Information Sharing Act* passed by Congress in 2015 (*CISA 2015*).

More recently, ITI developed policy recommendations designed to help the U.S. Congress, CISA, and other government stakeholders develop an effective and efficient cybersecurity incident reporting regime, including to support the *Cyber Incident Reporting for Critical Infrastructure*

[2] Executive Order 14028 on Improving the Nation's Cybersecurity (May 12, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[3] Visit https://www.itic.org/about/membership/iti-members for a full list of ITI members.

Act of 2022. I had the privilege of testifying before the House Homeland Security Committee in support of that bill, and ITI has subsequently been deeply engaged in providing comments as part of CISA's rulemaking process to help make sure that important law is effectively implemented. I commend this committee for its continued leadership on cybersecurity matters, and I would like to thank you and your staff for the thoughtful and deliberative approach you are taking in examining the CSRB and how it can best support the cybersecurity ecosystem.

After briefly providing important background regarding the importance of productively aligning the CSRB with CISA's partnership ethos to maximize the complementary role it can play within the existing network of public-private cybersecurity partnerships, the balance of my written testimony will focus on the two areas that ITI believes are most worthy of the Committee's careful deliberation as it considers the present utility and future value of the CSRB: 1) the **appropriate role, structure and governance of the CSRB,** including to **ensure both the independence of the CSRB and its board members and that they are selected through a clear and transparent process,** as well as to clearly articulate the **criteria and methodology for selecting which incidents the CSRB investigates**; and (2) recommendations on **maximizing the value of the CSRB in supporting the cybersecurity ecosystem**, including to ensure clear and appropriate **confidentiality, nondisclosure, and liability protections** for information provided during CSRB reviews.

Aligning the CSRB with CISA's Partnership Ethos

ITI has long advocated that public-private partnerships are essential to improving cybersecurity. CISA and its predecessor entities at the Department of Homeland Security have long been established as key partners to industry on issues such as cybersecurity threat information sharing and supply chain risk management. Public-private partnerships acknowledge that government and industry often have access to unique information sets and bring diverse experiences and perspectives to the table. Historically these partnerships have been essential to 1) identify potential threats; 2) understand how and to what extent risks can be managed; and 3) determine what actions should be taken to address risks without yielding unintended consequences.

The private sector ICT community has not only been foundational in developing the infrastructure of cyberspace but, for two decades, in providing leadership, innovation, and stewardship in all aspects of cybersecurity anchored in numerous public-private partnership structures and efforts. For example, global ICT companies have participated in the IT, communications, and other sector coordinating councils (SCCs), self-organized, self-governed councils that allow owners and operators of critical infrastructure to engage on a range of cybersecurity strategies, policies, and activities with CISA and other U.S. government counterparts. Global ICT companies also participate in several public-private partnership efforts sponsored by or housed at CISA, including: the ICT SCRM Task Force, a public-private partnership launched in 2018 and charged with identifying challenges and developing actionable solutions to enhance global ICT supply chain resilience; the Enduring Security Framework, a public-private partnership that addresses threats to critical infrastructure and National Security Systems; the NSTAC, a public-private advisory body developing industry-based, collaborative advice to help assure the availability, reliability, security and resilience of telecommunications services in the U.S.; and the Joint Cyber Defense Collaborative, an operationally-focused public-private partnership launched in 2021 that unites cyber defenders in the collaborative defense of cyberspace.

We believe that if the CSRB is crafted carefully and invested with the partnership ethos that is the hallmark of these other partnerships, it can serve as a durable, helpful, and complementary resource that provides an authoritative accounting and analysis of significant cybersecurity incidents. If structured under a partnership model the CSRB can increase awareness of the underlying factors that gave rise to such incidents and provide actionable recommendations to help avoid their recurrence. In order to realize the full potential of the CSRB, the Board must be firmly established as a trusted and collaborative partner to industry – in the same way CISA and its predecessors at DHS have engaged with relevant stakeholders, including critical infrastructure owners and operators, on the array of important and ongoing cybersecurity and supply chain risk management partnership activities referenced above.

Appropriately protecting sensitive business information shared during CSRB investigations is essential to aligning CSRB with CISA's partnership mission and ethos, as well as to incentivizing voluntary participation in CSRB investigations more broadly. Should the CSRB remain structured the way it is now – *i.e.*, including "non-federal" private sector representatives – we believe that the Charter or other CSRB organizational document should set clear parameters around the protection of business sensitive information, including to exempt information provided to the CSRB during the course of a review from Freedom of Information Act (FOIA) requests. ITI member companies strongly believe that any legislation codifying the CSRB should likewise make clear that materials acquired by the Board (both voluntarily provided or otherwise) are exempt from disclosure under FOIA and exempt from use in litigation and for regulatory purposes, including enforcement actions. This committee is familiar with existing models for providing such protections, such as the *CISA 2015* cybersecurity information sharing law, which included language exempting the information shared thereto from FOIA, for use in any lawsuits, and for regulatory purposes. [4] Mirroring such an approach for the CSRB will assure participants that information provided will be appropriately stored and protected, and that there are

[4] The widely discussed legislative proposal published by DHS contains similar protections for information provided voluntarily. *A Bill to Establish the Cyber Safety Review Board,* sec. 890G, https://www.cisa.gov/sites/default/files/2023-04/dhs_leg_proposal_-_csrb_508c.pdf.

appropriate guardrails around which information is released publicly, helping to better incentivize participation on the part of the private sector.

The Appropriate Role, Structure and Governance of the CSRB

ITI member companies believe that convening an independent body such as the CSRB that is focused on developing a shared, authoritative history and analysis of significant cybersecurity incidents can prove valuable to U.S. federal agency leadership, company management, and cybersecurity practitioners alike. CSRB reviews can positively impact the overall cybersecurity ecosystem by helping to elucidate the details of events which led to an incident and explain how it was remediated. After time has passed, CSRB reviews can retrospectively examine the real-world impacts of an incident, including whether response actions taken by the government or other actors had any impact on the malicious cyber actor(s) responsible. Published CSRB reviews can inform how organizations evolve their cybersecurity practices, policies, and threat response activities as well as how they prioritize and resource cybersecurity investments.

In order to realize the vision and harness the promise of the CSRB, it is critical that the structure and governance of the board is thoughtfully conceived. In our view doing so includes ensuring the independence of the Board and creating clear and transparent processes for selecting members of the Board and incidents for review.

(a) Independence of the CSRB

Deriving the full value of the Board requires that it be structured as an independent entity whose exclusive purpose is to serve as a resource – it should not be able to be used by other government agencies as a means of obfuscating or otherwise augmenting existing regulatory reviews or investigations. In this way, the CSRB can serve as a valuable resource and perform a complementary service to the IT ecosystem by providing in-depth retrospective reports and analyses of significant cybersecurity events, a function which does not otherwise exist today within the ecosystem of current U.S. security public-private partnerships or otherwise.

(b) Membership of the CSRB

As emphasized above, ITI and our member companies strongly believe in the value of public-private partnerships. However, ITI member companies are not of one-mind regarding the best way to approach industry or non-federal membership of the CSRB. Some ITI members have noted the value and imperative of industry involvement and expertise in CSRB activities. For instance, private sector cybersecurity firms have deep visibility – both through expansive sensor/tooling deployments and incident response efforts – into the global cyber threat landscape. This reality uniquely situates representatives from those entities, even if acting in their personal capacities, to bring aggregated and anonymized ecosystem-wide insights of enormous value to CSRB deliberations.

Other ITI members have expressed concerns about the potential for private sector participation in the CSRB to create real or perceived conflicts of interest, or the perception that competitive bias could influence the Board's activities. Policy makers should carefully consider this dynamic given the widely discussed public proposal to give the CSRB limited subpoena authority, which exacerbates these concerns.[5] While we understand that proposal sought to somewhat insulate non-federal members from decisions as to whether the CSRB should issues subpoenas, the fact remains that investing a CSRB with 50% of its members coming from the private sector with the power to subpoena competitors of those members' employers may shape the public perception of the CSRB in a way that undermines the objectivity and independence of the CSRB, as well as its partnership mission.

ITI member companies who expressed concerns over the composition of the CSRB offered a variety of potential solutions to ensure private sector participation without undermining the CSRB's credibility. For instance, one ITI member company proposed dividing the responsibilities for selecting incidents and the reviews themselves. Under this model an interagency panel would be empowered to select the incidents for CSRB review and investigation, while the actual analysis could be conducted by a more diverse body including private sector participation in some form.

Other ITI members suggested that policymakers may want to consider staffing the board's reviews exclusively with Federal employees to avoid the perception that the CSRB's analysis and findings are tainted by business interests. Following the example of the National Transportation Safety Board (NTSB), with which the CSRB has been compared,[6] policymakers could consider a small board of individuals with private sector backgrounds, each appointed by the President and subject to the Senate confirmation process, who oversee the CSRB's activities. The diversity of views amongst our membership on this issue suggests the need for careful deliberation and further solicitation of stakeholder views on the best approach to CSRB membership.

Beyond the issue of the board's composition, it will be critical to establish an open and transparent process for Board member selection. The Charter should lay out the specific criteria used to evaluate and select potential board members.[7] It will also be important to rotate the composition of the board by defining set terms for CSRB members, an approach reflected in the current Charter as well as the DHS legislative proposal, both of which contemplate two-year terms for CSRB members that are potentially renewable. Under this model, policymakers

[5] *Id*. at sec. 890F(c).

[6] Brook, Chris, *A Cyber NTSB: DHS Announces Cyber Review Board*, Feb. 3, 2022, Data Insider, https://www.digitalguardian.com/blog/cyber-ntsb-dhs-announces-cyber-review-board

[7] The current CSRB Charter contains scant detail regarding the criteria for selecting members from the private sector, other than that individuals from "appropriate cybersecurity or software suppliers" should be included. *See* Cyber Safety Review Board Charter, sec. 6, https://www.cisa.gov/sites/default/files/2023-09/CSRB%20Charter%2009.21.2023%20APPROVED_508c.pdf

should ensure the Board is comprised of stakeholders that represent a diverse set of backgrounds and professional expertise, including human factor specialists and privacy and security advocates, in addition to policy and technical security experts. Finally, the Charter should set forth a process for providing participants with advance transparency about which Board members will participate in a review, as well as specific criteria for recusal of a Board member in a given review and a process for participants in a review to request recusal of a specific Board member on the basis of specified criteria.

(c) Selecting Incidents for CSRB Review

Given the CSRB has only completed two reviews to date – the first on Log4j, the second on a series of attacks associated with a group of threat actors known as Lapsus$ – there is a limited body of work from which to draw definitive conclusions regarding the Board's functioning and impact. However, one of the challenges that we have noted with regard to the CSRB thus far is the lack of clarity regarding the process and criteria by which incidents are selected for investigation and review.

We understand that Log4j was a comparatively easy review from the perspective of gaining industry cooperation, given Log4j was an open-source vulnerability that affected thousands of people and organizations globally, few of which were under any type of investigation or regulatory scrutiny for their role in the event. Many organizations were pleased to cooperate with the Board's review. Indeed, a number of ITI member companies cooperated and participated in the Board's investigation into Log4J, and in fact some ITI member companies reported encountering difficulty contacting the Board to provide their perspectives. One preliminary conclusion we can draw from the selection of Log4j for the inaugural report that the widespread nature of the incident and other factors made gaining the cooperation of impacted or otherwise interested private sector entities relatively easy. Another is that the investigation of Log4j intuitively and objectively seems to rise to the level of "significant cyber incident." Indeed, CISA Director Jen Easterly referred to log4j as the "most serious" security vulnerability she had seen in her career.[8]

On the other hand, the investigation of Lapsus$ – a threat actor group – and its techniques does not intuitively seem to entirely fit into the definition of a "significant cyber incident." While investigating a threat actor group and its techniques may be useful, it is worth noting there are multiple federal agencies, including CISA, that individually or collectively regularly conduct and produce reports similarly focused on threat actors,[9] and so it is not clear that the CSRB deciding

[8] CNBC, Dec. 16, 2021, *CISA director says the LOG4J security flaw is the "most serious" she's seen in her career* [video file], https://www.cnbc.com/video/2021/12/16/cisa-director-says-the-log4j-security-flaw-is-the-most-serious-shes-seen-in-her-career.html

[9] For a recent selection of advisory reports published by CISA and various other federal and international cybersecurity partners, *see, e.g.,* Joint Cyber Advisory: IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors,

to take on this threat actor and group of incidents was necessarily a unique value add – even if some of the recommendations contained in the Lapsus$ report have in fact proved valuable and immediately actionable.[10] Based on the differences between the first report on Log4j – which fits more neatly into the definition of "significant cyber incident" – and the second report on Lapsus$ – which focuses on a threat actor as opposed to a specific incident – it is not overtly clear how the Board is interpreting the PPD-41 definition of "significant cyber incident"[11] and on what criteria they are selecting investigations.

EO 14028 provides some helpful guidance regarding the level of incident that should qualify as a "significant cyber incident" justifying review by the CSRB. Section 5(c) of the EO mandates that the establishment of a Cyber Unified Coordination Group (UCG) as provided by PPD-41 will trigger a CSRB review. UCG's are convened fairly infrequently and only in the case of what most would consider "no brainer" significant cyber incidents – such as log4j, which itself triggered a UCG as well as the initial CSRB review, as discussed above. Notably, sec. 5(d) of EO 14028 also mandated that the CSRB's initial review should take on a specific incident that prompted the establishment of a UCG in December 2020 – the SolarWinds incident, which most would also intuitively determine meets the significant cyber incident threshold, but which the CSRB declined to review. In contrast, none of the cyber incidents attributed to Lapsus$ triggered a UCG to our knowledge. While whether a UCG has been triggered should not be dispositive, the convening of a UCG nevertheless does provide a reliable barometer of the level of incident that should be required to trigger CSRB review.

In light of the above, policymakers should ensure that reviews of incidents are based on a specific, publicly released set of criteria which is developed in conjunction with stakeholders. We understand that the CSRB may potentially investigate any "significant cyber incidents" as

Including U.S. Water and Wastewater Systems Facilities, Dec. 14, 2023, https://media.defense.gov/2023/Dec/04/2003350920/-1/-1/0/CSA-IRGC-AFFILIATED-CYBER-ACTORS-EXPLOIT-PLCS-IN-MULTIPLE-SECTORS.PDF; Joint Cyber Advisory: Russian Foreign Intelligence Service (SVR) Exploiting JetBrains TeamCity CVE Globally, Dec. 13, 2023, https://media.defense.gov/2023/Dec/13/2003358237/-1/-1/0/JCSA-SVR-EXPLOIT-JETBRAINS-TEAMCITY-CVE.PDF; Advisory: Russian FSB cyber actor Star Blizzard continues worldwide spear-phishing campaigns, Dec. 3, 2023, https://media.defense.gov/2023/Dec/07/2003353251/-1/-1/0/ADVISORY-RUSSIAN-FSB-CYBER-ACTOR-STAR-BLIZZARD-CONTINUES-WORLDWIDE-SPEAR-SPHISHING-CAMPAIGNS.PDF.

[10] For example, last December the Federal Communications Commission (FCC) acknowledged the Cyber Safety Review Board's recommendations from the Lapsus$ review in issuing an enforcement advisory to prevent SIM swapping. FCC, Dec. 11, 2023, *FCC WARNS TELECOM COMPANIES OF OBLIGATIONS TO PROTECT ACCESS TO CONSUMERS' CELL PHONE ACCOUNTS AND SENSITIVE INFORMATION FOLLOWING DEPARTMENT OF HOMELAND SECURITY'S CYBER SAFETY REVIEW BOARD REPORT* [PRESS RELEASE], https://docs.fcc.gov/public/attachments/DOC-398998A1.pdf

[11] PPD-41 provides that the term "significant cyber incident" means: A cyber incident that is (or a group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interest, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. *Presidential Policy Directive -- United States Cyber Incident Coordination*, July 26, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

defined by PPD-41, but this is still a fairly expansive definition capturing significantly more potential incidents than those ultimately triggering UCG review. Additionally, limited information is publicly available as to how the Board interprets and applies this definition, despite the fact that EO 14028 additionally charges the DHS Sec. with prescribing "thresholds and criteria for the types of cyber incidents to be evaluated" by the CSRB in the future.[12] We believe that in order for the CSRB process to be as effective and credible as possible, clear scoping criteria regarding how incidents are selected for review is needed and should be publicly disclosed. One ITI member has offered that a potential way to initially scope the incident selection process and make it more efficient would be to limit CSRB reviews to the "covered entities" and "covered incidents" as defined by the implementing regulation of the *Cyber Incident Reporting for Critical Infrastructure Act of 2022* (CIRCIA) – however such an approach is premature given CISA has not yet defined those terms via the rulemaking process.

It is possible the CIRCIA rulemaking will result in a large number of cybersecurity incidents reported pursuant to CIRCIA, which would in turn generate a high-volume of events for the CSRB to potentially consider. So, if policymakers were to decide to leverage the definition and scope from CIRCIA to create an initial "pool" of events to consider for further review by the CSRB, additional criteria would nonetheless still be necessary to ensure an objective and fair process for deciding which subset of incidents warrant investigation by the Board.

Whatever the outcome of the CIRCIA rulemaking process, policymakers should consider developing a definition and criteria for a "significant incident" that clearly distinguishes the definition from the CIRCIA definitions. Policymakers should also develop a more nuanced and refined set of criteria to capture the types of impacts that will help to define "significant incident," including technical novelty, significant effects, impacts or harms in areas such as national security, and broader impacts on the IT, OT, or ICTS ecosystem(s). While we understand that the existing definition of "significant incident" used by the CSRB draws upon the definition in PPD-41, that definition is itself seems only focused on the potential impacts of cyber incidents, which as described are fairly expansive for the purpose of selecting the one or two incidents per year that may warrant CSRB-level review.

Further, whatever criteria are developed should be clearly articulated to ensure that potentially impacted stakeholders have awareness of the types of incidents that could give rise to a CSRB review. Emphasis on uniquely impactful cyber incidents will help to deconflict CSRB reports from the panoply of existing cybersecurity guidance, notifications, alerts, frameworks, advisories, general cybersecurity information sharing, and reports produced by other federal bodies and public-private partnerships. We stand ready to work with policymakers to help establish impactful evaluation criteria to define "significant incidents" moving forward.

[12] EO 14028, sec. 5(i)(v).

How the CSRB can Best Support the Cybersecurity Ecosystem

(a) Realizing the CSRB's Unique Value

Policymakers should consider how best to structure the Board's reports to provide unique value to public and private stakeholders in the security community. They should also consider what type of information is most useful to include in those reports. The Cyber EO established the CSRB to review and assess significant cyber incidents and make concrete recommendations for improving cybersecurity and incident response practices. In our view, the focus of the CSRB's activities should primarily be on reviewing, assessing, and analyzing those significant incidents, because no other body has such a focus. Of course, the CSRB should also fulfill its mandate by making recommendations to improve cybersecurity based on its reviews of significant incidents, but in doing so it should take care to distinguish any such recommendations from the recommendations, best practices, and guidance regularly produced by many other cybersecurity stakeholders, to ensure the CSRB is not duplicating the efforts of others.

Analyzing whether the CSRB's recommendations are impactful cannot be measured simply in terms of whether a particular recommendation in a report itself is intrinsically useful but should also be evaluated through the lens of whether other bodies are producing similar recommendations. CISA, the NSA, and FBI/DOJ routinely produce high-quality cybersecurity technical advisories, indicators of compromise, or other risk information, as referenced above. In addition to threat and vulnerability alerts, those same federal agencies produce guidance documents such as the Guidelines for Secure AI Systems Development[13] recently released by CISA and its UK counterpart, the ESF documents on best practices for Software Bill of Materials,[14] and frameworks such as the seminal NIST Cybersecurity Framework.[15] Additionally, other public-private partnerships and advisory committees involving one or more of these same federal agencies, such as the NSTAC and the ICT SCRM Task Force, also regularly produce recommendations and guidance documents on some of these same or similar topics.

Additionally, as the CSRB conducts additional reviews it will be important to conduct a retrospective of the CSRB's work. For instance, the GAO could periodically examine the Board's reviews and reports to understand the scope and effectiveness of its impact on the cybersecurity ecosystem.

[13] Alert: CISA and UK NCSC Unveil Joint Guidelines for Secure AI System Development, Nov. 26, 2023, https://www.cisa.gov/news-events/alerts/2023/11/26/cisa-and-uk-ncsc-unveil-joint-guidelines-secure-ai-system-development

[14] National Security Agency, Nov. 9, 2023, NSA and ESF Partners Release Recommended Practices for Software Bill of Materials Consumption [Press Release], https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3584895/nsa-and-esf-partners-release-recommended-practices-for-software-bill-of-materia/

[15] NIST Cybersecurity Framework Resources page at https://www.nist.gov/cyberframework

Ultimately, for the CSRB to provide unique value it needs to do more than produce the same types of work product being produced elsewhere by CISA and/or other federal partners and public-private partnerships.

(b) Prioritizing Information Protection Over Compulsory Processes

ITI members believe that the CSRB would not need an independent subpoena authority if the Board's scope were limited to those entities and incidents already covered under CIRCIA, which already provides CISA with subpoena authority for non-compliance. Additionally, investing the CSRB with subpoena authority also arguably undermines the partnership mission of CISA.

If the underlying rationale of the CSRB is to benefit the cybersecurity community and improve cybersecurity outcomes, policymakers may also want to consider incentives for participation in the Board's reviews. To ensure the greatest level of transparency and therefore the most efficacious outcomes for cybersecurity practitioners, policymakers should consider a limited liability protection for participating entities or a bar on the admissibility of CSRB findings in U.S. court proceedings. In our view it is premature to give the CSRB subpoena authority to compel private sector participation in reviews unless it can be demonstrated that incentivizing participation is not effective, at least unless some other adequate justification is provided.

Policymakers should also carefully consider the impacts of CSRB reviews and compulsory processes on potential, or ongoing, civil, or criminal court proceedings and regulatory actions. Increased interest in cyber issues over the past several years has created a range of existing mechanisms for the CSRB to leverage for its own discovery purposes. Notably, the October 2023 Securities and Exchange Commission complaint[16] against SolarWinds Corporation and its chief information security officer illustrate the significant new legal liabilities emerging with respect to cyber incidents.

The CSRB's work needs to maintain clear boundaries and protections on information shared with the CSRB. In addition, the CSRB must avoid conflicts of interest with law enforcement or regulatory agencies in order to maintain the credibility of reviews and not hamper participation in the Board's work, but this goal is compromised if there are unclear boundaries or protections around information that is shared during the course of a Board investigation. It will also be important for policymakers to monitor the health of the various public-private partnerships CISA maintains in the wake of its regulatory responsibilities under CIRCIA, but at present CISA remains a successful leader of public-private partnerships (*e.g.* through the Joint Cyber Defense Collaborative, Sector Specific Coordinating bodies, and the ICT SCRM Task Force) and accordingly CISA seems a viable home for the CSRB.

[16] Securities and Exchange Commission, Oct. 30, 2023, SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures [Press Release], https://www.sec.gov/news/press-release/2023-227

Conclusion

Members of the Committee, ITI and our member companies once again commend you for your longstanding leadership on cybersecurity issues and are pleased you are examining the CSRB and how it can most effectively play a valuable and complementary role in supporting the cybersecurity ecosystem.

The CSRB holds the promise and potential to deepen our understanding in the wake of significant cybersecurity attacks, raising the level not only of conversation but practices so as to avoid the successful recurrence of those attacks. To realize those benefits it will be important for Congress – both as a legislator and overseer – to ensure that CISA retains its unique role as a trusted, non-regulatory partner to the private sector and security community more broadly, and the CSRB is invested with this same ethos.

Today's hearing is a crucial step towards getting the CSRB concept right. As with this Committee's work on incident reporting, it will be imperative to take a thoughtful approach to the governance of the CSRB, its membership, and how incidents are chosen for review. ITI stands ready to provide the Committee with any additional input and assistance in the spirit of collaboration as you continue your efforts to fully realize the promise of the CSRB.

I thank the Chairman, Ranking Member, and Members of the Committee for inviting me to testify today and for their interest in and examination of this important issue. I look forward to your questions.

Thank you.