ISSUE BRIEF

FEBRUARY 2024

Future-Proofing the Cyber Safety Review Board

BY MAIA HAMIN, ALPHAEUS HANSON, TREY HERR, AND STEWART SCOTT

The **Cyber Statecraft Initiative** works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

The mission of the **Digital Forensic Research Lab (DFRLab)** is to identify, expose, and explain disinformation where and when it occurs using open-source research; to promote objective truth as a foundation of government for and by people; to protect democratic institutions and norms from those who would seek to undermine them in the digital engagement space; to create a new model of expertise adapted for impact and real-world results; and to forge digital resilience at a time when humans are more interconnected than at any point in history, by building the world's leading hub of digital forensic analysts tracking events in governance, technology, and security.

EXECUTIVE SUMMARY

The US government's Cyber Safety Review Board (CSRB) was established in a 2021 Executive Order to investigate complex cybersecurity failures and translate their lessons into recommendations to improve the nation's cyber safety. The work of the Board to date has revealed its potential but also illuminated how the organization will need to evolve to meet its loftiest goals and resist the vicissitudes of political calculus. This brief makes several suggestions for how codifying the Board in legislation should tackle key design decisions about the CSRB. These recommendations are informed by lessons from the young history of the CSRB as well as historical analogy to the National Transportation Safety Board (NTSB), the independent federal agency charged with investigating aviation and other transport accidents and serving as significant inspiration for the purpose, if not yet the structure, of the CSRB.

Some of these changes focus on how the CSRB can best conduct the three key phases of its work: incident selection; investigation; and reporting and recommendations. On incident selection, standardized public criteria for how the Board chooses whether to investigate a particular incident—and offering opportunities for public feedback on its decision-making— would help build trust with both lawmakers and the broader public, allowing the Board to explain systematically decisions like its controversial choice to not review the infamous Sunburst/SolarWinds breach. It is almost incumbent that the Board is vested with subpoena powers to compel information from uncooperative entities, or else risk remaining hamstrung in its ability to tackle hard cases. Finally, legislation should include explicit mechanisms that compel other government agencies to respond to CSRB recommendations—mirroring the structure that has allowed the NTSB to see many of its recommendations implemented by the Federal Aviation Agency and other federal offices.

Other recommendations in this issue brief address broader questions about the structure and bureaucratic home of the CSRB. These include the issue of membership: currently the CSRB has only part-time members who retain their "day jobs," unlike the NTSB and its full-time Commissioners. To balance the need for independence with the benefits of part-time members with high-level, current insight into industry or government, lawmakers should consider a hybrid

structure with some part- and some full-time members, as well as a robust public process for handling conflicts of interest. Similarly, the CSRB has benefited from its placement in the Department of Homeland Security (DHS) and should remain there in the near term. Lawmakers should consider how and when the Board could transform into an independent agency, similar to the NTSB's transition from under the Department of Transpiration after concerns arose from its position within the same Department as the FAA, the agency to which it often makes recommendations.

In all these structures, one of the most important capabilities for a future CSRB is a capacity for evolution. Digital systems evolve constantly, as do the risks created by the integration of these technologies in core economic, social, and political processes. The incidents the CSRB will be called on to do its work—make systematic inquiries to discover and examine facts— will only grow more complex and contested over time. It is essential that the CSRB can grow and mature alongside these challenges. Armed with the right tools and the right structure, an ever-evolving CSRB can help the nation learn from its cyber mistakes in service of building a more resilient, safer cyber future.

INTRODUCTION

Understanding how and why complex systems fail has always been difficult. Investigations into the lapses behind airplane crashes[1] or oil spills[2] can take years, and when systems cause harm—economic crises, wars, social upheaval—analysis and investigation can roll on for decades. In recent years the development pace of digital systems and their staggering intricacy have accelerated to an unprecedented degree. Sprawling software supply chains, labyrinthian cloud infrastructure, and an ever-expanding internet are woven together to form a constantly evolving mosaic of digital systems. The potential consequences of the failure of these systems grow every day as they are more closely integrated with the real world. Market forces that push firms to move quickly while declaiming liability compounds the challenge of ensuring safety—an issue that the current administration is grappling with.[3]

The Cyber Safety Review Board (CSRB) was born from one of these failures—the sprawling Sunburst/SolarWinds compromise—and offers a solution to the enormous public interest in improving the safety of digital systems by learning from their shortfalls.[4] This will require an impartial, comprehensive account of major cyber safety incidents and their larger, systemic context. No entity in the private sector is positioned or incentivized to do this work justice. Incident response firms must consider their relationships with current and former clients; compromised companies must manage their reputation, legal exposure, and shareholders; and all stakeholders lack the wide lens required to repeatedly and rigorously investigate connected risks in the systems they build, operate, and secure. Only a body insulated from both market tumult and government turnover can take the long view needed to better understand and mitigate these increasingly complex cyber risks.

Having only been established by an executive order in 2021, there is growing interest in further institutionalizing the CSRB, evidenced by a legislative proposal from the Department of Homeland Security (DHS)[5] to codify the CSRB into law as well as a recent hearing by the Senate Homeland Security and Governmental Affairs Committee on the same topic.[6] This momentum presents an opportunity for assessment—not of the quality of the Board's work to date but instead of how far it has yet to go to realize its potential.

This issue brief will briefly review the CSRB's current design and recent work before building upon these lessons to suggest how its next incarnation could be structured to achieve its mandate. The discussion is arranged according to the lifecycle of a CSRB investigation: how cyber incidents are selected for investigation; how incidents and their causal factors are investigated; and how recommendations stemming from investigations are crafted and tracked. The brief will then propose design features that would maximize the CSRB's ability to learn from and across cyber incidents, communicate its processes and findings, avoid conflicts of interest with both industry and government, and improve itself as an investigative body amid a rapidly changing cyber landscape.

1 "The Investigative Process," National Transportation Safety Board, https://www.ntsb.gov/investigations/process/Pages/default.aspx.

2 "Deep Water: The Gulf Oil Disaster And The Future Of Offshore Drilling - Report to the President (BP Oil Spill Commission Report)," National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, January 11, 2011, https://www.govinfo.gov/app/details/GPO-OILCOMMISSION.

3 Maia Hamin, Sara Ann Brackett, and Trey Herr, with Andy Kotz, "Design Questions in the Software Liability Debate," *Atlantic Council DFRLab*, January 16, 2024, https://dfrlab.org/2024/01/16/design-questions-in-the-software-liability-debate/.

4 "Deep Water: The Gulf Oil Disaster And The Future Of Offshore Drilling - Report to the President (BP Oil Spill Commission Report)."

5 "A Bill to Establish the Cyber Safety Review Board," CISA, https://www.cisa.gov/sites/default/files/2023-04/dhs_leg_proposal_-_csrb_508c.pdf.

6 US Congress, Senate, Committee on Homeland Security and Government Affairs, The Cyber Safety Review Board: Expectations, Outcomes, and Enduring Questions, 118th Congress, 2nd session, 2024, https://www.hsgac.senate.gov/hearings/the-cyber-safety-review-board-expectations-outcomes-and-enduring-questions-2/.

WHAT'S IN A CYBER SAFETY REVIEW BOARD?

The Story of the CSRB So Far

Executive Order (EO) 14028 established the CSRB in response to the Sunburst/SolarWinds incident[7] with the mandate to "review and assess…threat activity, vulnerabilities, mitigation activities, and agency responses" related to "significant cyber incidents…affecting FCEB [Federal Civilian Executive Branch] Information Systems or non-Federal systems."[8] The Board consists of one government representative each from the Department of Defense, the Department of Justice, the Cybersecurity and Infrastructure Security Agency (CISA), the Department of Homeland Security (DHS), the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), and the Office of the National Cyber Director (ONCD)—as well as an optional representative from the Office of Management and Budget (OMB) for incidents affecting FCEB systems. Currently, seven industry representatives from firms such as Google, Palo Alto Networks, Verizon, and others also serve as Special Government Employees on the Board.[9] This group convenes at the discretion of the President or the Secretary of Homeland Security, as well as any instance when a cyber incident leads to the establishment of a Cyber Unified Coordination Group (UCG), such as in the wake of the Sunburst/SolarWinds campaign.[10]

Once the CSRB concludes a report it follows a standard dissemination process. The Director of CISA provides the CSRB's report to the Secretary of Homeland Security, who then passes the full version of the investigation to the President before making an unclassified version available to the public. So far, the CSRB has published reports covering the Log4j incident and the Lapsus$ criminal group, and it is currently working on a review of the July 2023 Microsoft cloud security incident.[11] The Board also produced a self-assessment covering its early work, which included recommendations for changing its design.[12]

Early Investigations

The CSRB's first review covered the Log4j incident, where a vulnerability in a ubiquitous open source software library offered attackers crippling access to a large number of affected systems. The investigation revealed important information, such as the fact that there was no evidence the vulnerability had been exploited before the disclosure, and made recommendations such as addressing ongoing risks from the vulnerability; driving best practices for security, vulnerability management, and software development; improving the cohesion of and visibility into the larger software ecosystem; and bolstering longer-term investments in security. While the inaugural report received widespread praise from cybersecurity commentators,[13] certain concerns lingered. For one, the fact that the Board's report was released so close to the public announcement of the Log4j vulnerability positioned it as something closer to incident response than the Board's notional goal of incident review, emphasized by the public acknowledgment from CISA of the exploit of Log4j within a federal agency more than four months after the Board's report and uncovered during CISA's incident response engagement.[14] Additionally, the report's recommendations were notably broad, which is somewhat understandable given the Board's novelty at the time and the sprawling reach of Log4j, but worth considering in terms of practicality.[15]

The Board's second report covered Lapsus$, a criminal group that utilized familiar but highly effective social engineering tactics to launch a series of high-profile attacks against several large companies.[16] The Board's decision to focus on Lapsus$ received more mixed reviews than its first investigation. Some experts critiqued the utility of reviewing a group that was already known and studied by the industry (its direct victims) and clearly in the remit of government's Joint Ransomware Task Force.[17] These critiques prompted increased calls for transparency in the Board's incident selec-

7 For more on this incident, see Trey Herr, Will Loomis, Emma Schroeder, Stewart Scott, Simon handler, and Tianjiu Zuo, "Broken Trust: Lessons from Sunburst," Atlantic Council, March 29, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/broken-trust-lessons-from-sunburst/.

8 "Executive Order on Improving the Nation's Cybersecurity," The White House, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

9 "Cyber Safety Review Board (CSRB) Members," CISA, https://www.cisa.gov/cyber-safety-review-board-csrb-members.

10 "CYBERSECURITY: Federal Response to SolarWinds and Microsoft Exchange Incidents," Government Accountability Office, January 2022, https://www.gao.gov/assets/720/718495.pdf.

11 "Department of Homeland Security's Cyber Safety Review Board to Conduct Review on Cloud Security," US Department of Homeland Security, August 11, 2023, https://www.dhs.gov/news/2023/08/11/department-homeland-securitys-cyber-safety-review-board-conduct-review-cloud.

12 "Cyber Safety Review Board of Inaugural Proceedings," CISA, October 18, 2022, https://www.cisa.gov/resources-tools/resources/cyber-safety-review-board-inaugural-proceedings.

13 Tom Uren, "Srsly Risky Biz: Thursday July 21," *Seriously Risky Business*, July 20, 2022, https://srslyriskybiz.substack.com/p/srsly-risky-biz-thursday-july-21.

14 "Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvester," CISA, November 25, 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-320a.

15 Uren, "Srsly Risky Biz: Thursday July 21."

16 "Review Of The Attacks Associated with Lapsus$ And Related Threat Groups Report," CISA, August 10, 2023, https://www.cisa.gov/resources-tools/resources/review-attacks-associated-lapsus-and-related-threat-groups-report.

17 "Joint Ransomware Task Force," CISA, https://www.cisa.gov/joint-ransomware-task-force.

tion process.[18] The report on Lapsus$ included recommendations for covering securing identity and access management (IAM) systems, managing vulnerabilities specific to telecommunications firms and their resellers, making business process providers more resilient, better coordinating law enforcement responses, and disincentivizing cybercrime.[19]

The Board's most recent investigation focuses on an incident from the summer of 2023 in which a threat actor exploited flaws in Microsoft's cloud infrastructure to access government information systems, including the email accounts of senior officials.[20] The cloud industry and its increasingly important yet opaque systems are well worthy of review, and the announcement drew praise from experts.[21] The involvement of a major industry player such as Microsoft, and the potential takeaways for other cloud firms, also meant that this investigation was the first in the Board's history to see instances of voluntary Board member recusal due to conflicts of interest.[22]

Lessons Learned

Certain key questions about the current design and function of the CSRB provide useful insight into potential next steps for the Board as an institution. The first is how well the CSRB has lived up to its envisioned purpose. Here, one divergence looms large: the absence of an investigation into Sunburst/SolarWinds. That incident was the impetus for the CSRB's creation and the first incident it was explicitly asked to review; that attack also led to a cyber UCG, a criterion that would have triggered a review under the CSRB's current charter. Rob Silvers, Undersecretary for Policy at DHS, argued the lack of an investigation into Sunburst/SolarWinds was due to a difficult tradeoff, stating that "the White House and the Department of Homeland Security together determined that when the board was launched, that at that point in time, the best use of the board's expertise and resources was to examine the recent events involved in the Log4j vulnerability."[23] Cyber commenters have speculated about additional potential rationales for the decision, including that it would have cast an unwelcome light on the state of government cybersecurity or that it would have been impractical for an institution without subpoena power to investigate such a high-profile attack.[24] That these factors may impact the Board's willingness and ability to examine important incidents highlights key design considerations for a codified CSRB. Potential concerns around the CSRB scrutinizing government cybersecurity highlight its need for eventual independence and challenges around the compliance of entities with its reviews necessitate strengthened investigatory tools.

Perhaps the greatest missed opportunity of the absent Sunburst/SolarWinds investigation is the chance for the CSRB to investigate not just singular incidents but larger patterns of compromise and their context. **Abuse of Microsoft identity and access management (IAM) systems played a significant role in the Sunburst/SolarWinds campaign**.[25] These are the same linchpin technologies likely to play a starring role in the Board's forthcoming examination of the role of cloud services in threat actor Storm-0558's breach of Microsoft and several government agencies in the summer of 2023 (which also resembled SolarWinds in the intelligence-gathering motivations of the perpetrators).[26] These architectural flaws illustrate the importance of the Board's ability to impartially examine singular, complex incidents as well as across multiple breaches with common traits.

A second question in evaluating the current Board is its progress toward driving the adoption of its recommendations. Assessing this question is difficult, in part because adoption within the industry is opaque and not easily measured. In some cases, the Board appears to have already spurred change. See, for example, Federal Communications Commission (FCC) Chairwoman Jessica Rosenworcel saying simply, "the Cyber Safety Review Board…recommended that we take action to support consumer privacy and cut off these [SIM-swapping] scams. That is exactly what we do today," regarding recent FCC requirements and guidance.[27] In other instances, though, the impact of the Board's recommendations is far less clear. Since the Log4j report, open source software has gained more explicit support in government and industry, evidenced by initiatives such as CISA's OSS Roadmap[28] and the ONCD's Open-Source Software Security Initiative. However, these projects have yet to come into full force, and related legislation, such as the Securing Open-Source Software Act, remains unenacted. Similarly, the

18 John Sakellariadis, "With Lapsus$, Cyber Review Board Draws Mixed Reviews," *Politico*, December 5, 2022, https://www.politico.com/newsletters/weekly-cybersecurity/2022/12/05/with-lapsus-cyber-review-board-draws-mixed-reviews-00072144.

19 "Review Of The Attacks Associated with Lapsus$ And Related Threat Groups Executive Summary," CSRB, https://www.cisa.gov/sites/default/files/2023-08/Review%20Of%20The%20Attacks%20Associated%20with%20Lapsus%24%20And%20Related%20Threat%20Groups%20Executive%20Summary_508c.pdf.

20 "Department of Homeland Security's Cyber Safety Review Board to Conduct Review on Cloud Security."

21 A. J. Vicens, "Cyber Safety Review Board to Analyze Cloud Security in Wake of Microsoft Hack," *CyberScoop*, August 11, 2023, https://cyberscoop.com/cyber-safety-review-board-microsoft-cisa-dhs/.

22 Heather Adkins (@argvee), "Today, CISA's Cyber Safety Review Board announced it will review Cloud Security and assess the recent Microsoft intrusion. Given scope of this study, I have recused myself from the Board's review," X, August 11, 2023, https://twitter.com/argvee/status/1690015584740687872.

23 Mariam Baksh, "Cyber Safety Review Board Closes the Book on SolarWinds While Reporting on Log4j," *NextGov*, July 14, 2022, https://www.nextgov.com/cybersecurity/2022/07/cyber-safety-review-board-closes-book-solarwinds-while-reporting-log4j/374220/.

24 Jeff Stone, "US Cyber Review Punts on Russian Hack, Hinting at Limitations," *Bloomberg,* November 16, 2022, https://www.bloomberg.com/news/newsletters/2022-11-16/us-cyber-review-punts-on-russian-hack-hinting-at-limitations.

25 Herr et al., "Broken Trust: Lessons from Sunburst;"

26 Trey Herr, "Three Key Unanswered Questions about the Chinese Breach of Microsoft Cloud Services." *CyberScoop*, July 20, 2023, https://cyberscoop.com/microsoft-cloud-breach-china/.

27 Jessica Rosenworcel, "Protecting Consumers from SIM Swap and Port-Out Fraud, WC Docket No. 21-341, Report and Order and Further Notice of Proposed Rulemaking," FCC, November 15, 2023, https://docs.fcc.gov/public/attachments/FCC-23-95A2.pdf.

28 "CISA Open Source Software Security Roadmap," CISA, September 12, 2023, https://www.cisa.gov/resources-tools/resources/cisa-open-source-software-security-roadmap.

recent proposal[29] from the Department of Defense, General Services Administration, and NASA to reform the Federal Acquisition Regulation to require that contractors develop and maintain software bills of materials largely aligns with the Log4j report's recommendations, but the proposal itself points more directly toward EO 14028 as its source. As such, recent action around open-source software and software supply chain security might well have stemmed from the Log4j and Sunburst/SolarWinds incidents themselves more so than the CSRB's reporting.

THE CSRB OF THE FUTURE

What is the unique value that the CSRB offers as an investigative entity? In short, the CSRB has the opportunity to serve as a non-partisan, independent, and deeply transparent organization that studies the underlying causes and context of cyber incidents, threats, risks, and trends. This is essential for unpacking the complex causal chains that create cyber failures, which, in turn, is a prerequisite for informing and developing cyber risk management policies and practices informed by the complexity of real-world cases. The CSRB's investigations should be factual accounts from which it can identify and recommend policies and practices to improve cybersecurity and safety outcomes for US citizens, national security, industry, and key allies and partners alike. In doing so, the Board should also evaluate and draw lessons from the relationships between the individual cases of their reviews, evaluating risk and safety in the interconnected cyber ecosystem. It should also track and analyze the progress of the implementation of its recommendations, including their impact, lessons learned, and roadblocks, in service of improving itself as an institution.

No other entity in the cyber ecosystem can replicate this set of functions. Many organizations have reasonable incentives to hide information related to the causes of their failures and even, sometimes, their existence. Self-investigation by government or industry carries obvious motivations—financial, legal, and reputational—to mitigate fault finding, or at least its public reporting. Incident response firms are focused on recovery rather than review and are subject to market forces, the need to appease clients, and time pressures not conducive to systemic analysis. Law-enforcement efforts, meanwhile, are more geared toward proving criminal liability rather than exposing the full picture of an incident. The limited liability structures for cybersecurity failures in the US mean that such cases are often brought on the basis of fraud, where an entity misrepresented its security practices, rather than examining all factors contributing to an incident or its broader context.[30] Such investigations are not designed to produce concrete policy recommendations and understandably disincentivize transparency.

The Cyber Safety Review Board was inspired in significant ways by lessons learned from safety investigations in other domains, particularly in aviation and transportation.[31] In these sectors, one agency in particular bears a remarkable similarity to the mission and the design of the CSRB: the National Transportation Safety Board (NTSB). The NTSB is an independent agency charged with investigating a significant portion of transportation incidents, including but not limited to aviation accidents and failures. It produces factual, impartial accounts of complex failures that inform (often remarkably specific) recommendations, many of which are implemented by industry and government. It enjoys a large full-time staff, access to industry experts, and a stable budget, carrying subpoena power but effectively no regulatory authority. Moreover, the NTSB specifically tracks the status of its most-desired policy changes as well as which of its recommendations government and industry implement over time.[32]

These are all useful designs for the CSRB to draw from. However, the subject mandated to the CSRB—cyber safety—bears some important differences from the NTSB's. The information covered in CSRB analysis (such as digital products or sensitive government systems) raises far more concerns about confidentiality than airplane crashes or train derailments. Frustratingly, the consequences of cybersecurity failures are often less directly connected to their source, too, with hard-to-quantify and widespread knock-on effects such as intelligence compromise and private-sector revenue losses. The very systems the CSRB must investigate are also much more complex and are intertwined with seemingly countless facets of industry and society, as well as with one another. And unlike the familiar world of transportation regulation, the CSRB's domain changes rapidly and unexpectedly depending on new technology and vulnerabilities, all while the CSRB remains a nascent government agency with still-growing institutional processes and expertise. The following recommendations address both divergences and similarities between the CSRB and NTSB.

29 "Federal Acquisition Regulation: Cyber Threat and Incident Reporting and Information Sharing," Federal Register, October 3, 2023, https://www.federalregister.gov/documents/2023/10/03/2023-21328/federal-acquisition-regulation-cyber-threat-and-incident-reporting-and-information-sharing.

30 "SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures," SEC Press Release, October 30, 2023, https://www.sec.gov/news/press-release/2023-227.

31 Robert Knake, Adam Shostack, and Tarah Wheeler, "Learning from Cyber Incidents: Adapting Aviation Safety Models to Cybersecurity," Belfer Center for Science and International Affairs, November 12, 2021, https://www.belfercenter.org/publication/learning-cyber-incidents-adapting-aviation-safety-models-cybersecurity.

32 "Safety Recommendations," NTSB, https://www.ntsb.gov/investigations/Pages/safety-recommendations.aspx.

The Lifecycle of a CSRB Investigation

The lifecycle of a CSRB investigation provides a useful structure for addressing different design questions that arise at each stage. The next sections are structured according to this model.

- **Incident selection**: The incidents that the CSRB selects for review should support the Board's broader goal of identifying causes of cyber failure to inform impactful changes in policy and practice. Its processes for doing so should prioritize transparency and trust-building to help policymakers and the public understand its criteria and how they are applied.

- **Incident review**: To investigate cyber incidents in enough depth to understand their complex causes and illuminate practices and policies that could have prevented or limited their associated harms, the CSRB will require the authority to access a significant amount of information. To build trust with potential parties in the investigation, from the private sector to the government itself, the Board should also establish procedures to ensure it safely handles the information it obtains. The Board's membership structure will need to balance the need for independence against the benefits of closer integration with industry and government, containing robust public processes for navigating conflicts of interest and recusals.

- **Recommendations**: The CSRB's main vehicle for improving cyber safety is its recommendations. Its structures and processes for making recommendations should focus on driving efficacy without the need for regulatory authorities, such as legal requirements for other agencies to respond to the Board's recommendations. Additionally, the Board itself should be responsible for tracking its recommendations and the progress other agencies and the private sector have made toward implementation.

Other considerations, such as about the CSRB's location within the executive branch, cut across all three phases and are consolidated in their own section at the end of this issue brief.

Incident Selection

The process for the CSRB's selection of incidents for review should be designed, from the outset, to maximize the Board's success at identifying causes of cyber failure and ways to increase cyber safety through their remediation.

Currently, the President and the Secretary of Homeland Security can nominate incidents for CSRB review, and the Board also considers incidents that lead to the formation of a Cyber UCG. Once confirmed through one of these channels, the Board has the ultimate authority to decide which incidents to prioritize. This structure works well but could be augmented by explicitly allowing members of the Board to nominate incidents as well. This pathway would be especially useful if the CSRB's capacity is expanded—a recommendation made in later sections—allowing the Board to potentially pursue multiple investigations simultaneously.

Greater changes are needed to the process of deciding whether to launch an investigation for a nominated cyber incident. Currently, the CSRB makes these decisions in private according to non-public criteria. This should change. In its legislation, Congress should develop criteria for incident prioritization or require the CSRB itself to determine and publicize an independent set of standards. A public set of criteria for incident selection would serve several purposes.

The first is simply that such transparency creates the opportunity for public debate and comment on the factors that the CSRB uses to select cyber incidents. Public criteria would allow Congress or other stakeholders to advocate for changes to better align the CSRB investigative process with its mission and address the lack of trust that can accompany opaque reporting processes. In recognition of the utility of public input, as well as the fact that the Board itself may learn additional factors it considers important in the selection process, Congress should build a mechanism for the Board to update these standards.

Second, these public criteria can be useful as the Board justifies its decision-making on specific cases. For example, when the Board selects a case, it can publicly defend its decision in terms of how it stacks up against its selection criteria. This would establish a common understanding of an incident's significance and contribute to driving cross-incident analysis. Also, these standards would provide useful common ground for discussions of the reasons that an incident was *not* reviewed. If the Board consistently evaluates major cyber incidents against its selection criteria, it could publicize its reasoning for not taking up a particular incident in response to Congressional or public inquiries (as have persisted regarding Sunburst/SolarWinds) in a more prominent, consistent format.[33] This is not to cast doubt on the Board's intentions or methods but instead to build in, with the force of law, a standard and an obligation for transparent reasoning and to continually develop trust in the Board's judgment.[34]

The following incident criteria, while overlapping significantly with each other and reflecting much of the Board's extant thinking, are a useful start. These criteria should not preclude other triggers for investigation, such as the formation of a cyber UCG or the discretion of the President or the Secretary of Homeland Security.

33 Vicens, "Cyber Safety Review Board to Analyze Cloud Security in Wake of Microsoft Hack."
34 Sakellariadis, "With Lapsus$, Cyber Review Board Draws Mixed Reviews."

- **Severity of harm**: The magnitude and reach of an incident's harm to US citizens and national interests, as well as the potential for ongoing impact if the initial incident remains unaddressed.

- **Incident generalizability:** The likelihood that the failure could generalize to other systems or organizations if left unaddressed, for example, due to the effect an incident has on some common piece of technology or core digital infrastructure, or because the failure implicates widespread organizational practices.

- **Policy context:** The degree to which an incident reveals potential flaws in policy, such as existing requirements that were unenforced or ineffective at preventing an incident, or where relevant policy controls were simply nonexistent.

- **CSRB context:** The relevance of the incident to previous CSRB investigations and nominated incidents, striving to capture incidents that are indicative of larger systems issues while avoiding duplicative work.

Incident Investigation

The CSRB should not be a punitive entity, but it also should be unflinching in its questioning and analysis. Only an agency with the proper authorities, independence, and powers will be able to conduct the hard analyses critical to the CSRB's broad mission of improving cyber safety in the national interest.

At present, the powers the Board has at its disposal have limitations. Cooperation with Board investigations is voluntary, as the body cannot issue administrative subpoenas. Legislative codification should grant the CSRB subpoena authority akin to the NTSB's. Without the ability to compel the production of information, the Board cannot gather data from companies or branches of government that decline to cooperate, severely hamstringing its ability to tackle some of the most important cases. These cases may pertain to sensitive systems, flagrant negligence, or other features an entity would understandably want to keep hidden from the public.

DHS's proposed legislation usefully pairs the ability of the CSRB to make requests for voluntary responses with subpoena powers for non-compliant entities. The proposal cleverly provides an additional incentive for disclosure by protecting voluntarily disclosed information from being used as the basis for enforcement actions or otherwise used in civil litigation, while offering no such protections for subpoenaed information.[35] Ultimately, the CSRB's investigations should largely resemble its current process with the addition of subpoena power and DHS's reasonable proposal to waive actions taken against voluntarily disclosed information.

One factor that significantly distinguishes the NTSB from the CSRB is the NTSB's stated policy to hand off an investigation to local law enforcement or the FBI should an accident be determined to have been a criminal act.[36] This focuses the NTSB's activities on failure and accident rather than premeditated malice. The CSRB, in contrast, will need to and has already investigated incidents where digital systems are compromised by a malicious party. For this reason, the CSRB, by design, cannot and should not hand off incidents simply because they were caused by a malicious criminal act. To maximize its success at improving cyber safety, and to avoid duplicating law enforcement and public-sector investigations of specific cyber threat actors, the CSRB should focus more on the causes and conditions that lead to cyber insecurity rather than on the perpetrators of cyber harm.

Report and Recommendations

The final stage of a CSRB investigation is the creation of a report on the incident. This report should describe the causal chain of the failure and the lessons learned, which are then translated into recommendations for the private sector and policymakers.

How the CSRB formulates its recommendations and ensures implementation is a key challenge for a body without regulatory authority. Again, the development of the NTSB offers instructive lessons. The NTSB works closely with regulators within the Department of Transportation (DOT) like the FAA to implement its recommendations. This close collaboration is backstopped by a hard legal requirement for the DOT and its constituent agencies to respond to NTSB recommendations within 90 days. Because of this requirement, agencies like the FAA have established uniform procedures for responding to NTSB requests.[37]

Likewise, federal agencies addressed in CSRB recommendations should be required to respond to the investigation's recommendations within 90 days. This written response should include an assessment of the feasibility of implementing the recommendations and a plan of action to respond to the report. This would include agencies that contribute to federal government cyber security, such as the Department of Homeland Security (including CISA), the Office of Management and Budget, and the General Services Administration. It would also include agencies that regulate the cyber practices of certain critical infrastructure sectors, such as the Department of Health and Human Services (healthcare and public health sector) and the Department of Treasury (financial services sector).

As the CSRB continues to review, report, and recommend, it will develop a larger body of recommendations, and more evidence will become available on their implementation status. The Board's codification in law should also require

35 CISA, "A Bill to Establish the Cyber Safety Review Board."

36 NTSB, "The Investigative Process."

37 "Order 1220.2G - FAA Procedures for Handling National Transportation Safety Board (NTSB) Recommendations," FAA, May 13, 2011, https://www.faa.gov/documentLibrary/media/Order/1220.2G.pdf.

the CSRB itself to systematically track its recommendations and their degree of implementation (or lack thereof), much as the NTSB does.[38]

It is essential that CSRB continue to released publicly its investigations to inform the decision-making of private sector entities as well as government. Sometimes, in the course of its work, the CSRB will need to interact with classified information. The CSRB should have an obligation in law to formulate its reports and recommendations, to the maximum extent possible, to be publicly releasable while avoiding the publication of classified information. Where the Board decides that achieving the goals of a report necessitates describing classified information or creating recommendations that would necessitate classification, it should formulate both a classified and unclassified version of the report and release the latter publicly. Similarly, the CSRB will need to interact with plenty of confidential business information during its investigations. The CSRB's first obligation should always be to the public by relaying critical information and recommendations. However, it should minimize the extent to which its final reports reveal confidential private-sector information beyond what is required to achieve its mandate.

Structure of the Board

Membership

The efficacy of the CSRB as an institution will rely heavily on the makeup of the Board. Board members will play several key executive oversight and functional roles throughout the full lifecycle of an investigation. The CSRB's membership would ideally maximize both its independence and its investigative and recommendation capacity throughout these phases. However, these two goals point in slightly different directions.

To strike a balance between the two, codifying legislation should establish that the Board be composed of half full-time members and half part-time members from industry, with the chair position held by a full-time member. The full-time Board members would buoy the CSRB against conflicts of interest and provide significant investigative capacity as well as the potential for institutional knowledge, while the part-time members would ensure the Board's proximity to and professional currency in the technology systems it must investigate. The presidential appointment of one full-time member as Board chair (and thus the tiebreaking vote) would further mitigate the influence of conflicts of interest.

Conflicts of interest arising from part-time Board membership, if unmanaged, could severely harm the integrity and value of the Board's work as well as its reception. Current government employees serving on the Board might be disincentivized to find fault with their own agency's oversight for fear of negative ramifications in their current role or relationships. Private-sector employees might avoid investigating their own employer for similar reasons or seek out opportunities to investigate competitors. Yet, a Board with current government or private sector employees also creates notable advantages concerning its capacity. Primarily, this allows the Board to attract senior and experienced members who might otherwise be disinclined to resign from their current positions—the same individuals who have contemporary expertise on the underlying technologies that the CSRB investigates. A blended model of full- and part-time members would help to balance these advantages and costs. With both full- and part-time members having equal voting power, there would always be sufficient "independent" votes to select potentially controversial or far-reaching (but important) cases, all while preserving the benefits of increased expertise and connectivity available through the part-time model.

Even with such a hybrid model, the CSRB must have a well-developed and publicly documented process for handling conflict-of-interest recusals. The Board's current recusal process, per recent comments made by DHS Undersecretary for Policy Rob Silver, involves DHS ethics lawyers reviewing members' financial disclosures and, for each case, conflicting incentives.[39] While this structure's broad contours are reasonable, the details of the process and the criteria by which lawyers make their judgments about the threshold for recusal should be made public by the CSRB. Documentation of this process will build trust among policymakers and the public that conflicts of interest cannot threaten the integrity of the CSRB's selection, investigation, and recommendation processes. As such, lawmakers should require the Board itself to develop and publicize this process and the relevant criteria. Board members should have the opportunity to recuse themselves from certain parts of the life cycle of an investigation, from the initial vote to the investigative and recommendations processes, as each of these activities may create different potential conflicts of interest.

Regardless of the constitution of the Board itself, the CSRB as an organization should have a budget for more full-time investigative staff. Between the accelerating pace of cyber incidents and the demands of rigorous investigations, limiting CSRB resources to just a few full-time employees is a disservice to its mission and the importance of the public interest of its investigations. The NTSB, for example, has hundreds of full-time staff and can draw on more from across industry and government. While the structure of the CSRB does not need to be identical to that of the NTSB—part of the strength of the CSRB is that Board members participate more in actual investigations—increasing its number of full-time staff will allow the CSRB to respond to a greater number of cybersecurity incidents while treating each with appropriate care. Eventually, the goal should be to build the Board's capacity to the point where it can perform more than one investigation at the same time, similar to the NTSB.

38 NTSB, "Safety Recommendations."

39 Patrick Gray and Adam Boileau, "Risky Business #733 -- Say cheese, motherf---er," *Risky Business*, January 24, 2024, https://risky.biz/RB733/.

Finally, lawmakers should codify the explicit authority for the Board to bring in external experts to assist with particular cases, mirroring the "party system" of the NTSB, which "enlists the support and oversees the participation of technically knowledgeable industry and labor representatives who have special information and/or capabilities" in its investigations.[40] If included, this should be a privilege of the Board itself, rather than a right afforded to the Secretary of Homeland Security as the current DHS-proposed legislation suggests.

Finding a Home

The prospect of legal codification offers an opportunity to consider whether the CSRB's current position within DHS is the best possible structure for its long-term success. The CSRB has benefitted thus far from its proximity to agencies and departments with considerable resources and expertise, as well as from the ability to utilize DHS's broader infrastructure for the various operational and administrative tasks required of a federal organization. Eventually, though, the goal should be to transform the CSRB into an independent agency, similar to the trajectory of the NTSB.

The NTSB began as an agency within the Department of Transportation (DoT). Yet, it often investigated policies and actions of the FAA, a fellow DOT agency, creating natural conflicts of interest. Several years after its creation, Congress addressed these foundational questions by establishing the NTSB as an independent agency.[41]

When the CSRB investigates compromised FCEB systems and critical infrastructure providers, it must look to the role of fellow DHS entity CISA, which is responsible for helping FCEB agencies and critical infrastructure providers manage their security and cyber risk. So long as the Board is housed within DHS, this risks creating conflicts of interest between the Board and the agency in which it resides (and upon whose infrastructure it relies for day-to-day operations). Because different critical infrastructure sectors work with a variety of Sector Risk Management Agencies, simply finding a different departmental host for the CSRB is liable to create similar risks. Thus, in the long term, the Board should become an entirely independent agency.

What is less clear is whether this transition should occur in tandem with the Board's legislative codification or whether the CSRB should follow a similar path to NTSB and become independent only once it is more established. Standing up the resources needed for a new, independent agency is difficult and so may be reasonable grounds to table the issue for another few years while the CSRB develops into a full-fledged investigative body with significant resourcing.

It is also important to note that the future independence of the CSRB does not require the Board to sever ties with CISA or DHS. The NTSB and the FAA still investigate in tight coordination and with significant cooperation, but the NTSB has sufficient independence to both inform and critique the FAA's decisions.[42] So too must the CSRB have the freedom to speak, directly and honestly, to all other parts of the government, while still working alongside the agencies most affected by its decision-making.

Evolution

Part of the CSRB's key contribution to cybersecurity is its ability to consider failures across the ecosystem in connection with each other, from a position that affords long-term analysis rather than immediate response. The CSRB should be required to perform additional forms of meta-review in support of this end. For example, Congress could require, at regular intervals, a report from the CSRB on its past findings and the connections among the systems it investigates—a synthesis report. Similarly, the CSRB should be required to collect and examine recommendations that have gone unimplemented and assess the likely causes of inaction. This information can also help inform Government Accountability Office (GAO) investigations, which have long found and attempted[43] In addition, the Board should be explicitly empowered to revisit and revise reports when new information comes to light after their investigation. Several of these functions might be delegated to CSRB subcommittees, which are already established in its charter.

Along with these meta-reviews, the CSRB should also have mechanisms for required self-review. Congress should require the CSRB to review its structure and make recommendations to Congress on potential reforms every five years. This would include ways to refine its case selection criteria, membership structure, budget and staffing, and investigative procedures—as well as a self-assessment of how well the Board is meeting its mandate. Such mechanisms would vest Congress with a key decision-making role over the CSRB and would provide means for ongoing adaptation of the structure and function of the Board.

Congress cannot and should not expect to remake the CSRB in the NTSB's image in a single legislative act. Yet, neither should it be satisfied with a similar decades-long timeline of growth. The threat landscape is too fast-changing, and the stakes of failure in the cyber domain are too high. In short, policymakers will need to design a Board that can and must iterate and improve over time.

40 "What Is the National Transportation Safety Board?" NTSB, https://www.ntsb.gov/about/Documents/SPC0502.pdf.

41 "History of The National Transportation Safety Board," NTSB, https://www.ntsb.gov/about/history/pages/default.aspx.

42 "Failure of FAA to Implement NTSB Recommendations Contributed to Fatal Air Tour Helicopter Crash, NTSB Says," NTSB, May 10, 2022, https://www.ntsb.gov/news/press-releases/Pages/NR20220510.aspx.

43 "Cybersecurity: NIH Needs to Take Further Actions to Resolve Control Deficiencies and Improve Its Program," Government Accountability Office, December 7, 2021, https://www.gao.gov/products/gao-22-104467.

CONCLUSION

The creation of the CSRB, and the efforts towards its enshrinement into law, reflect an understanding and a commitment from the federal government: addressing the challenges created by the proliferation of digital systems across every facet of society will necessitate self-examination and self-improvement. Fact-finding among the complexities, interrelationships, jargon, finger-pointing, and sales pitches of the cyber ecosystem is a challenging task, and the CSRB is the only entity custom-built to tackle it.

The CSRB is developing at a crucial moment, as industry- and government-led mechanisms to improve the accountability and security of digital vendors have begun to bloom. Examples include mechanisms like the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) and the Security and Exchange Commission's welcome public-disclosure rules, as well as the voluntary use of software bills of material by some of the most cybersecurity-mature organizations and the adoption of similar requirements in public-sector contracts. The CSRB's findings have a clear audience. Over the next decade this network will grow further, magnifying the influence of the Board's investigations and findings.

In light of the importance of the CSRB's mission, as well as the importance of this moment in the wider cybersecurity ecosystem, questions about its design and operation are critical. It is rare to face the opportunity to stand up a policy structure from scratch, at the right moment, with widespread expert enthusiasm, and with helpful past lessons at hand—and all the more important to get it right as a result. The suggestions raised in this issue brief to illustrate how legislative codification can make the body even more effective than it is today. The Board can become more transparent and participatory in its selection of incidents while increasing its investigative and fact-finding capacity. It can also interact in more meaningful ways with the many other organs of government tasked with managing a piece of the cyber puzzle, maximizing its efficacy as an agent of change while managing conflicts of interest.

The challenges ahead in this domain, and the difficulty of understanding how to ensure the safety and resilience of ever-more complex systems will only grow. Policymakers now have the opportunity and the challenge to create a CSRB that can meet this consequential moment while having the ability to evolve to tackle the risks and dynamics of the future.

ABOUT THE AUTHORS

Maia Hamin is an Associate Director with the Atlantic Council's Cyber Statecraft Initiative. She works on the intersection of cybersecurity and technology policy, including projects on the cybersecurity implications of artificial intelligence, open-source software, and cloud computing. Prior to joining the Council, Maia was a TechCongress Congressional Innovation Fellow serving in the office of Senator Ron Wyden, and before that a software engineer on Palantir's Privacy and Civil Liberties team. She holds a BA in Computer Science from Princeton University.

Alphaeus Hanson is an assistant director with the Atlantic Council's Cyber Statecraft Initiative. Prior to joining the Council, Hanson was the inaugural security fellow at Krebs Stamos Group (KSG). As an analyst at KSG, he managed its policy portfolio and drafted feedback on National Institute of Standards and Technology space cybersecurity guidance. He earned a Bachelor of Science degree from the University of Delaware at the Alfred Lerner School of Business and Economics and a foreign language certificate in Spanish.

Trey Herr is the director of the Atlantic Council's Cyber Statecraft Initiative and an assistant professor of Cybersecurity and Policy at American University's School of International Service. At the Council, the CSI team works at the intersection of cybersecurity and geopolitics across conflict, cloud computing, supply chain policy, and more. Previously, he was a senior security strategist with Microsoft handling cloud computing and supply chain security policy as well as a fellow with the Belfer Cybersecurity Project at Harvard Kennedy School and a non-resident fellow with the Hoover Institution at Stanford University. He holds a PhD in Political Science and BS in Musical Theatre and Political Science.

Stewart Scott is an associate director with the Atlantic Council's Cyber Statecraft Initiative under the Digital Forensic Research Lab (DFRLab). He focuses on software supply chain risk management and open source software security policy. He earned his BA from Princeton University at the School of Public and International Affairs along with a minor in Computer Science.

Atlantic Council

Board of Directors

**Executive Committee Members*

List as of January 1, 2024