Testimony of

Dr. Trey Herr
Director, Cyber Statecraft Initiative
Atlantic Council

Before the
United States Senate
Committee on Homeland Security and Governmental Affairs

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

January 17th, 2024

Chairman Peters and Ranking Member Paul, members and staff of the Committee, thank you for the invitation to join you today. My name is Trey Herr. I serve as an Assistant Professor with American University's School of International Service and lead the Cyber Statecraft Initiative at the Atlantic Council, a non-partisan think tank based here in Washington.

In service of this useful conversation, I want to share several thoughts on the nature of the Cyber Safety Review Board, with an aim to identify its unique purpose and significant potential value. It is important to recognize that the Cyber Safety Review Board, CSRB for sake of brevity, of today is not the fulsome or final version of the board. First version of a civil aviation investigations body was created in the 1920s and its current incarnation didn't emerge until the 1970s. Significant battles were waged over the membership, size, and independence of what we now know as the National Transportation Safety Board and it is both necessary and useful that similar debates apply to the CSRB.

Understanding how and why systems fail has always been difficult. Investigations into the lapses behind airplane crashes [1] or oil rig spills[2] can take years, and when complex systems cause harm—economic crises, wars, social upheaval—analysis can roll on for decades. In recent decades the pace at which we build digital systems and their staggering complexity have accelerated to historically unprecedented degrees. Sprawling software supply chains, mammoth cloud infrastructure, and an ever-expanding internet are constantly reweaving into a system of complex systems. The potential consequences of their failure grow every day as they are more closely integrated with the real world. Compounding the deep challenge of ensuring safety while relying on these systems are market forces that push firms to move quickly to market, all while declaiming liability for disruption—an issue that the current administration is grappling with.

The Cyber Safety Review Board (CSRB) was born from one of these failures—the sprawling SolarWinds compromise—and offers a response to the enormous public interest in improving the safety of digital systems by learning from their shortfalls.[3] That activity requires 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 status with current and former clients, compromised companies must manage reputation and legal exposure to shareholders and regulators while all lack the luxury of the wide lens required to repeatedly and rigorously investigate the risks born from the connections between the systems they build, operate, or secure. Government, too, is not immune to the challenges of self-investigation.[4]

Proposed legislative action surrounding CSRB (the proposal to codify it into law from the Department of Homeland Security[5] highlight the opportunity for assessment—instead of whether or not the Board's work to date has been exemplary, but rather of how far it has to go to realize its potential, how to get there, and where that optimal point sits. The Board will face uniquely complex challenges year after year—systems failures shaping the malfunction or abuse of other systems. Only a body insulated from market tumult and government turnover can take the long view needed to better understand, and mitigate, these risks.

[1] https://www.ntsb.gov/investigations/process/Pages/default.aspx

[2] https://cybercemetery.unt.edu/archive/oilspill/20121211005728/http://www.oilspillcommission.gov/sites/default/files/documents/DEEPWATER_ReporttothePresident_FINAL.pdf

[3] https://www.washingtonpost.com/opinions/2020/12/15/enough-is-enough-heres-what-we-should-do-defend-against-next-russian-cyberattacks/

[4] https://www.alpa.org/news-and-events/air-line-pilot-magazine/accident-investigation

[5] https://www.cisa.gov/sites/default/files/2023-04/dhs_leg_proposal_-_csrb_508c.pdf

This testimony will briefly recap CSRB's design and recent work before comparing its current form to what it could be and discussing design features that maximize its ability to: learn from and across cyber incidents, communicate its findings and its investigative process from incident selection to final publication, function independent of conflicts of interest from both industry and government, and improve itself and its processes over time.

What's in a Cyber Safety Review Board?

Executive Order (EO) 14028 established CSRB in response to the SolarWinds incident 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."[6] The Board consists of one government representative each from the Department of Defense (DoD), the Department of Justice (DoJ), 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 join them, from firms such as Google, Palo Alto Networks, Verizon, and similar—serving as Special Government Employees, potentially subject to signing NDAs.[7] This group convenes at the discretion of the President or the DHS Secretary, as well as any time a cyber incident leads to the establishment of a Cyber Unified Coordination Group (UCG), as in the wake of the SolarWinds campaign, for example .[8]

The Director of CISA provides this group's report to the DHS Secretary, who passes it on to the President in full, before making permissible versions of the report available to the public whenever possible—those versions only contain non-classified, publicly available information barring explicit permission from concerned entities. So far, CSRB has published two reports publicly, covering the Log4j incident and the Lapsus$ criminal group, and it is currently working on its review concerning July 2023's Microsoft cloud security incident.[9] The Boards has also produced a self-assessment covering its early work and recommending changes to its design.[10]

CSRB's first review covered the Log4j incident, where a vulnerability in a ubiquitous open source software library offered attackers crippling access to a huge number of affected systems. The inaugural report received widespread praise from cybersecurity commentators.[11] Lingering concerns included the proximity in time of the review to the underlying incident, which seemed to border closer to incident response than the Board's notional goal of incident review, and the broadness of its recommendations—understandable features given the Board's novelty, the vulnerability's sprawling reach, and the abstract nature of cybersecurity incidents compare to aviation disasters, the common analogy stemming from the CSRB's similarities to and modelling on the National Transportation Safety Board with its more specific

[6] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[7] https://www.cisa.gov/cyber-safety-review-board-csrb-members

[8] https://www.gao.gov/assets/720/718495.pdf

[9] https://www.dhs.gov/news/2023/08/11/department-homeland-securitys-cyber-safety-review-board-conduct-review-cloud

[10] https://www.cisa.gov/sites/default/files/2023-04/cyber_safety_review_board_review_of_inaugural_proceedings_508c.pdf

[11] https://srslyriskybiz.substack.com/p/srsly-risky-biz-thursday-july-21

recommendations.[12] The report recommended addressing ongoing Log4shell risks; 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 toward security.

The Board's second report covered Lapsus$, a criminal group that utilized familiar but highly effective social-engineering tactics to launch a series of high-profile attacks against several large companies.[13] The Board's decision to focus on Lapsus$ received more mixed reviews than its first report. Some critiqued the utility of reviewing a group so well-known and focused on by industry, its direct victims in this case, and a topic already covered by existing government bodies like the Joint Ransomware Task Force.[14] Others asked for more transparency in the incident selection process to better understand the decision and establish the Board as maximally transparent.[15] The resulting report included recommendations covering securing identity and access management (IAM) systems, better managing vulnerabilities specific to telecommunications firms and their resellers, making business process providers more resilient, better coordinating law enforcement responses, and better disincentivizing cybercrime.[16]

The Board's newly announced investigation focuses on a recent incident in which a threat actor exploited flaws in Microsoft's cloud infrastructure to access government information systems including the emails of high-ranking officials.[17] The cloud industry and its labyrinthine, increasingly critical, systems are worthy of this scrutiny and the announcement drew some praise, tempered mainly by the desire to see the final report before casting judgment.[18] The selection also saw the first instances of voluntary Board member recusal.[19]

The Story of CSRB So Far

In evaluating how CSRB has fared up to this point, two key questions provide useful insight into next steps for the Board as an institution. First, is how well the CSRB has lived up the concept for which it was established in EO 14028, and one shortcoming looms large: the absence of an investigation into SolarWinds, the very incident that prompted the CSRB's creation, that it was explicitly ask to review, and that led to a UCG , which would have triggered a CSRB review had the group existed at the time. There are more useful lessons here than chiding, too. Two speculative rationalizations for the decision not to review SolarWinds are that it would have cast an unwelcome light on the state of government cybersecurity or that it would have been impractical for a Board lacking the subpoena power necessary to compel useful

[12] https://www.belfercenter.org/publication/learning-cyber-incidents-adapting-aviation-safety-models-cybersecurity

[13] https://www.cisa.gov/sites/default/files/2023-08/CSRB_Lapsus%24_508c.pdf

[14] https://www.cisa.gov/joint-ransomware-task-force, https://www.politico.com/newsletters/weekly-cybersecurity/2022/12/05/with-lapsus-cyber-review-board-draws-mixed-reviews-00072144

[15] https://www.politico.com/newsletters/weekly-cybersecurity/2022/12/05/with-lapsus-cyber-review-board-draws-mixed-reviews-00072144

[16] 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

[17] https://www.dhs.gov/news/2023/08/11/department-homeland-securitys-cyber-safety-review-board-conduct-review-cloud, https://www.bloomberg.com/news/articles/2023-08-11/microsoft-s-role-in-email-breach-to-be-part-of-us-cyber-inquiry

[18] https://www.darkreading.com/cloud-security/microsoft-cloud-woes-inspire-dhs-security-review, https://cyberscoop.com/cyber-safety-review-board-microsoft-cisa-dhs/

[19] https://twitter.com/argvee/status/1690015584740687872

evidence.[20] The former highlights starkly the need for the mechanical independence of CSRB, and the latter the consideration of what investigatory tools CSRB has at its disposal.

Perhaps most compelling though is the opportunity that a SolarWinds investigation would provide for CSRB to begin investigating not just singular incidents but their relationship with other patterns of compromise and their collective contexts. Abuse of Microsoft identity and access management (IAM) systems in Azure Active Directory played a massive role in the SolarWinds campaign[21]—the very same linchpin technologies CSRB speaks to in its Lapsus$ report, and both in products similar to and toward the same intelligence-gathering ends as are likely to be subject of the Board's forthcoming cloud security report.[22] This summarizes two significant value the Board offers—the ability to look impartially at complex incidents *as well as across them*.

A second question to evaluate the Board is the progress of its recommendations adoption. Assessing all those it has made so far is difficult, in part because adoption within industry is opaque and not easily measured, and in part because of the partial implementation of some aspects of these recommendations. In some cases the Board appears to have already made progress with its audience, with 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.[23]

In other instances though, causality is far less clear. In the wake of the Board's Log4j report, open source software has gained more explicit support in government and industry, evidenced by initiatives such as CISA's OSS Roadmap,[24] ONCD's Open Source Software Security Initiative, and more. However, these initiatives have yet to come into full force, and related legislation such as the *Securing Open Source Software Act* remains conspicuously absent. Similarly, the recent proposal[25] from the DoD, the General Services Administration, and NASA to reform the Federal Acquisition Regulation to require that contractors develop and maintain software bills of materials where applicable harkens to the Log4j report's recommendations, but the proposal itself points more directly toward EO 14028. In general, the recent action around open source software and software supply chain security in government and industry might well have stemmed from the Log4j and SolarWinds incidents themselves more so than CSRB's report on the former.

As the CSRB continues to review, report, and recommend, it will develop a larger body of recommendations, and more evidence will become available about whether its prior recommendations have been implemented in practice or policy. The Board's codification in law should reflect the importance

[20] https://www.bloomberg.com/news/newsletters/2022-11-16/us-cyber-review-punts-on-russian-hack-hinting-at-limitations

[21] https://www.atlanticcouncil.org/in-depth-research-reports/report/broken-trust-lessons-from-sunburst/#explained

[22] Rather than pointing the finger at Microsoft, this argument focuses on the unique opportunity to review, across incidents, the role of key technologies in systems sold and operated by a small number of vendors to organizations with extraordinary security needs and threat models.

[23] https://docs.fcc.gov/public/attachments/FCC-23-95A2.pdf

[24] https://www.cisa.gov/resources-tools/resources/cisa-open-source-software-security-roadmap

[25] https://www.federalregister.gov/documents/2023/10/03/2023-21328/federal-acquisition-regulation-cyber-threat-and-incident-reporting-and-information-sharing

of assessing this critical metric by requiring the CSRB itself to systematically track its recommendations and their degree of implementation (or lack thereof), much as the NTSB does.[26]

The Board versus Existing Authorities

It's worth stepping back to evaluate what unique value CSRB can offer as an investigative entity and how its progress toward that abstract function is to date. CSRB should serve as a non-partisan, impartial, and deeply transparent entity to study the underlying causes and context of cyber incidents, threats, risks, and trends. Its investigations should be factual accounts, from which CSRB can identify and recommend policies essential to improving cybersecurity and safety outcomes for US citizens, national security, industry, and key allies and partners. In doing so, the Board should also look to evaluate and draw lessons from the relationships between the subjects of their reviews, evaluating risk and safety in the interconnected cyber ecosystem in a manner critical for improving the domain's safety. It should also track progress against meeting its recommendations, analyzing both reasons for their stalling where applicable, their impact where implemented, and ways to improve itself as an institution.

No other entity in the ecosystem can replicate this set of functions. Cybersecurity is complex and sprawling, a domain where many entities face incentives to hide information about the causes of their failures. 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, meanwhile, are focused on recovery rather than review and are subject to the business cycle, the need to appease clients, and time pressures not conducive to systemic analysis.

Law-enforcement efforts, meanwhile, aim to prove a civil or criminal case more than to determine the full picture of an incident. The existing limited structure of liability for cybersecurity failures in the US means that such cases are most often brought on the basis of false claims or fraud where an entity misrepresented its security practices rather than examining all factors contributing to an incident or their broader context. Such criminal (and civil) investigations are not structured to produce policy recommendations.

Analysts often point to the NTSB as a useful model for CSRB, and one with a far longer history.[27] Indeed, it is an independent agency charged with investigating a specific, significant portion of transportation incidents, including but not limited to aviation. 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, the ability to tap on industry experts, and a stable budget. It carries subpoena power but no regulatory authority. It tracks its most-desired policy changes as well as which of its recommendations government and industry implement over time.[28]

These are all useful designs for CSRB to draw from and on which this document will elaborate. However, the subject mandated to CSRB—cyber safety—bears some important differences than the NTSB's. Far more of the information covered in CSRB analysis of digital products and sensitive government systems raises concerns about confidentiality. The consequences of cybersecurity failures are often less directly connected to their source.[29] The very systems CSRB must investigate are far more complex and diverse, intertwined with many more facets of industry and society, and connected more deeply and opaquely with

[26] https://www.ntsb.gov/investigations/Pages/safety-recommendations.aspx

[27] https://www.cfr.org/blog/cyber-safety-review-board-should-investigate-major-historical-incidents

[28] https://www.ntsb.gov/investigations/Pages/safety-recommendations.aspx

[29] How explicitly can one assess the harms caused by an enormous volume of intelligence compromise or the trickling impact of massive revenue loss?

each other. The CSRB's domain is changing much more rapidly and unexpectedly, and the entity itself is far younger. The following recommendations address these divergences as well.

The Once and Future CSRB

Codification of the Board through legislation should help it drive better security by shedding light on past incidents and the connections among them to produce recommendations for policy and practitioners. The ongoing legislative discussion around CSRB should focus far less on assessing the adequacy or suitability of its two reports to date and much more on their ability to inform its future trajectory toward the state described above.

In codifying the structure of the Board in law, Congress has a role to play in learning from these past experiences and using these lessons to inform structural changes. Congress should prioritize legislative structures to address the selection of incidents for Board review, the conduct and dissemination of these reviews, the Board's membership and staffing, its synthesis of reports, its place among government offices and agencies, and its capacity for continued evolution.

Incident Selection

In its codification, CSRB should develop an independent set of criteria for its selection of incidents. Each review should discuss the reasons that an incident was selected in terms of how it stacks up against these criteria (though codification should require the Board to continually assess and update those criteria). Such a practice would establish a common understanding of an incident's significance and contribute, mechanically, to driving cross-incident analysis.

Separate of the reasons that an incident was *not* reviewed might also provide useful transparency and insight into the adequacy of the Board's incident selection criteria. 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, as other commenters have suggested.[30] 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 SolarWinds).[31] Proactively defining standards for the types of cyber incidents the Board must review might not be desirable, given the challenge of creating a standard that balances completeness against the feasibility and time costs of performing and publishing evaluations. However, Congress could selectively exercise this right in its oversight capacity, such as by asking the CSRB to provide its evaluation against their public criteria when it believes that an important incident has gone uninvestigated. The selection standards should also be made public to reinforce the transparency of the entire process. The decision for or against investigating a specific entity should be understandable and available for the general public.

The following incident criteria for selection of an incident for review, while overlapping significantly with each other and reflecting much of the Board's extant thinking, are a useful start (and they should not preclude other causes for investigation, such as the formation of a UCG or the discretion of the president or the DHS secretary):

- Missing practices that would have prevented or mitigated a compromise or its consequences;

[30] https://www.politico.com/newsletters/weekly-cybersecurity/2022/12/05/with-lapsus-cyber-review-board-draws-mixed-reviews-00072144

[31] https://cyberscoop.com/cyber-safety-review-board-microsoft-cisa-dhs/

- The ability of an incident to impact core digital infrastructure and destabilize the wider digital ecosystem;
- The potential for ongoing or future harm in absence of policy change;
- The complexity of an incident and its relationships to others, reviewed previously or not, especially when compounding its consequences;
- The severity and reach of an incident's harm to US citizens and national interests;
- The failure of existing policy or regulation directly relevant to the incident to *cover* causes of an incident;
- The failure of existing policy or regulation to *prevent or substantially limit the harms of* an incident where it reasonably should have done so; and
- The applicability of recommendations derived from review of an incident to drive broader security and safety improvements.

Incident Review and Reports

CSRB should not be an entity that is punitive in its investigations, but it does need to be unflinching in its questioning and analysis. Codifying law should require the Board to submit all reports to the public. As a body whose principle value is its investigative output, the audience for which is wide and public, the board should not receive or hold classified information. Government agencies working to support the Board's work are better positioned to declassify and share such information than the Board would be to try and preserve a twin track 'high' and 'low' investigative and reporting process. Transparency in the process of reporting to the public substantiates the work CSRB does, and industry is too fundamental a part of the cyber ecosystem to be excluded from recommendations if they are to be practical and helpful. More broadly, CSRB must become a trustworthy organization, one which does not punish but is ruthless in its analysis. Creating such an environment will require some hard investigations, which only an impartial and transparent entity can with appropriate powers can undertake successfully.

Only an entity with the proper authorities and powers will be able to conduct the hard analyses critical to CSRB's fulfilling its mission of improving cyber safety. At present, the powers the Board has at its disposal have limitations. Cooperation with Board investigations is voluntary, as the body lacks the ability to issue administrative subpoenas. Legislative codification should grant CSRB subpoena authority akin to the NTSB's. Without the ability to compel the production of information, the Board cannot gather information from companies or branches of government that decline to cooperate, severely hamstringing its ability to tackle some of the most important cases, which might pertain to sensitive systems, flagrant negligence, or other features an entity would understandably want to keep hidden. DHS's proposed legislation usefully pairs the ability for the CSRB to make requests for voluntary responses with the ability to subpoena entities that are not compliant. It cleverly provides an additional incentive for voluntary disclosure by protecting voluntarily-disclosed information from being used as the basis for an enforcement action or in civil litigation against the entity who disclosed (with no such protections for subpoenaed information). [32]

Importantly though, the Board's recommendations should not have the force of regulation or law, nor do they need to. Creating such powers would clash with other US government cyber authorities and detract from the Board's impartiality while straining its expertise with the additional burden of policymaking. Neither should CSRB's authorities transgress existing cyber policy such as the Cyber Incident Reporting for Critical Infrastructure Act and the SEC's cyber incident disclosure rules—CSRB is not an entity to which incidents must be immediately disclosed, but instead one that can work in complement to these requirements by taking up investigations of incidents that have already been disclosed or publicized under

[32] https://www.cisa.gov/sites/default/files/2023-04/dhs_leg_proposal_-_csrb_508c.pdf

these powers. The NTSB functions effectively without regulatory authority. Investigations ultimately should resemble CSRB's current process, with the addition of information that can only be gained through subpoena, and the DHS's proposals for the circumstances under which one would be requested are reasonable.

The Board must also implement measures to treat sensitively the information it collects through investigation. The NTSB does not investigate criminal matters, indeed its findings are not treated as a replacement for discovery in civil litigation. [33] Under the proposed legislation, CSRB similarly removes information provided to it from future regulatory or judicial action. This is important as under such a logic, both the NTSB and CSRB are intended to determine the causes of an incident and how to mitigate it but neither is charged with determining fault. Regarding proprietary or confidential information, CSRB should be required to minimize the extent to which its final reports reveal business confidential information beyond what is required to effectively deliver its findings and recommendations, lest such disclosures disincentivize cooperation from industry or government.

Investigating Criminal Acts

This gives rise to a slightly different factor which does distinguish NTSB from the CSRB. The NTSB's stated policy is to hand off an investigation to local law enforcement or the FBI should an accident be determined to have been a criminal act.[34] This focuses the NTSB's activities to circumstances of failure and accident rather than premeditated malicious act. Where the probable cause is malice, it is logical to transfer the investigation. The CSRB by contrast will need, and has already begun, to investigate incidents where digital systems are compromised by a purposeful and malicious party *but where significant questions still exist about how the compromise was possible*.

Many incidents with complex causes, insecurities, and design flaws not apparent to operators or designers, will be eligible for CSRB review. Most of these may also involve a malicious party but in cybersecurity, there remains much to understand about the means by which a digital system can be made to do something its designers did not intend. Where CSRB focuses on the systems in question, their designs, flaws, and failures, it will execute an important mission for which there is no competing authority. If CSRB focuses on the actors and their motivations or tactics or intent – it gives up a unique role and becomes competitive with myriad private and public sector entities doing the same thing. CSRB can maintain this important link with the scope and purpose of NTSB's activities by focusing on flaws and failures in the system of interest.

Membership

The lifecycle of the CSRB is important to any discussion of membership. From incident selection, through investigation, to finalizing recommendations, each step is critical and depends upon the previous section. The board's incipient step will be selecting an incident based on criteria such as those above. Following a thorough investigation, the CSRB would issue general recommendations or suggestions based on their findings, to improve the practices of related entities, or to move policy towards an ideal state. The CSRB's recommendations can pertain to regulatory bodies, private sector entities, operators of FCEB information systems, or a combination of the listed options. An integral aspect of remediation and improvement following the board's investigation of a cyber event is the drafting of these recommendations. Applying the findings of an investigation to both private sector entities and Federal Civilian Executive Branch Information Systems substantiates the value CSRB provides to the broader ecosystem. Finally, the board

[33] https://pilot-protection-services.aopa.org/news/2017/may/01/the-impact-of-ntsb-reports-in-civil-litigation

[34] https://www.ntsb.gov/investigations/process/Pages/default.aspx

can go further to track the implementation status of the recommendations they offered regarding a specific incident.

The efficacy of the CSRB as an institution will rely heavily on the proper makeup of the Board. Board members of the CSRB will perform several key executive oversight and functional roles throughout the lifecycle of an investigation, from selecting an incident for investigation, to conducting the investigation and drafting the report recommendations and (we suggest) overseeing the status of such recommendations' implementation. CSRB's membership would ideally be designed to maximize both its independence and its investigative and recommendation capacity throughout these phases. However, these two goals point in slightly different directions.

To maximize the Board's independence, lawmakers could choose to constitute it from only full-time members, similar to the makeup of the NTSB and in contrast with the current structure of the CSRB in which members are drawn from both industry and government and serve on the CSRB alongside their other role. Such a structure would mitigate (though not wholly alleviate) concerns about potential conflicts of interests that could arise if Board members need to vote on or be involved in investigation processes that relate to their current place of employment: 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, as private-sector employees might avoid investigating their own employer for similar reasons or seek out opportunities to investigate competitors to advantage their company's market position. On the other hand, allowing the Board's members to be current government or private sector employees also creates notable advantages with respect to the capacity of the Board. Primarily, it allows the Board to attract senior and experienced members who might otherwise be uninclined to resign their current positions, individuals who are likely to have highly current expertise on the technology and operations of either the private sector or the government. It also ensures that the Board remains relatively connected to other organs of government and to the private sector, potentially helping with the implementation of its recommendations.

Instead of picking one model or the other, lawmakers could seek to get the best of both worlds by codifying a hybrid structure, such as a Board with one half full-time and one half part-time membership, with a full-time, President-appointed Chair (who could also serve as a tiebreaking vote, if needed). Under such a model, both full and part-time members would have equal voting power concerning the Board's discretionary powers, including on the selection of cases. By selecting a half-and-half model, lawmakers would ensure that there would always be sufficient "independent" votes to select potentially controversial or far-reaching (but important) cases, while preserving the benefits of increased expertise and connectivity available through the part-time model.

Under any of these models, for both full-time and part-time members, the Board must have a well-developed and publicly documented process for handling conflict-of-interest recusals. Such a process is vital to retain the public perception of the Board's integrity as well as the actual integrity of its selection, investigation, and recommendation processes. Lawmakers should require the Board itself to develop this process and to publicly release its criteria and process for recusals. Board members should have the opportunity to recuse themselves from different parts of the life-cycle of an investigation, from the vote to begin it, to the actual process of the investigation, to the formulation of recommendations, as these different points might create different potential conflicts.[35]

[35] https://www.ntsb.gov/about/Documents/SPC0502.pdf

CSRB as an entity should be budgeted for an expanded staff to conduct these investigations. Between the accelerating pace of cyber incidents and the demands of rigorous investigations, limiting CSRB resources to just five full-time employees is a disservice to the important public interest its investigations serve. The NTSB, for example, has hundreds of full-time staff members. 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 processes such as the actual investigation—increasing its number of full-time staff will allow the CSRB to respond to a greater volume of cybersecurity incidents while treating each in depth, including potentially allowing the Board to perform more than one investigation at the same time, as does the NTSB.

Finally, law makers should codify the explicit authority for the Board to bring in outside 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 NTSB investigations.[36] If included, this should be a privilege of the Board itself, rather than a right afforded to the Secretary of the Department of Homeland Security as the current proposed DHS legislation suggests.

Synthesis and Evolution

Part of CSRB's key contribution to cybersecurity is its ability to consider cybersecurity failures across the ecosystem in conversation with each other, from a position of relative stability and over long timeframes. Codifying legislation can ensure this through three additional CSRB reviews. It should require, at regular intervals, a report from CSRB on its past reports with its past reviews and the connections among the systems it investigates in mind—a synthesis report. Finally, at a similar regular interval as its synthesis reports, CSRB should look at those recommendations that have gone unimplemented and assess the likely causes of that inaction. This information might also help inform GAO investigations, which have long found and attempted to explain lagging agency implementation of cybersecurity controls and policies.[37] In addition, the Board should be explicitly empowered to revisit and revise reports when new information comes to light after their publication. Several of these functions might be delegated out to CSRB subcommittees, which are already designed in its charter.

Formalizing the CSRB in law should build in explicit mechanisms for the Board to evolve over time. For example, Congress could require that, every five years, CSRB must review its own structure and make recommendations to Congress on potential updates, such as ways to evolve its criteria for case selection, the structure of its membership structure, its budget and staffing, or its investigative procedures—as well as its self-assessment of how well it is meeting its mandate. Such recommendations would ultimately put Congress in a deciding role but would provide means for ongoing adaptation in light of known and discovered best practices along the way.

Congress should not expect to remake CSRB in the NTSB's image in one legislative act, but neither should it be satisfied with a similarly decades-long timeline of growth, either in the face of a fast-moving threat landscape or with the NTSB's lessons in hand. Ensuring and codifying the Board's permanence cannot occur without also architecting a capacity for and forcing function to iterate and improve over time.

[36] https://www.ntsb.gov/about/Documents/SPC0502.pdf

[37] https://www.gao.gov/assets/gao-22-104467.pdf, https://www.gao.gov/assets/d24105658.pdf, https://www.gao.gov/products/gao-19-384, ad nauseam

Finding a Home

Finally, Congress should consider whether CSRB's current position within DHS is tenable in the long term. While CSRB's early days require proximity to agencies and departments with considerable resources, insight, and infrastructure, ultimately it should strive for true independence in line with the NTSB's own history. NTSB began as an agency with the Department of Transportation (DoT), where it often investigated the role of the Federal Aviation Administration, a fellow DOT agency, which led to an act of Congress establishing its independence from the DoT a few years later.[38] In the same vein, when CSRB investigates compromised of FCEB systems, it in part must look at the role of fellow DHS entity CISA, responsible for helping FCEB agencies manage their security and cyber risk. However, an prospective independence for CSRB need not sever the ties between the CISA or DHS and the Board—NTSB and the FAA still investigate in tight coordination and with significant cooperation but the NTSB has sufficient independence both to inform, and critique, the FAA's decisions.[39]

Conclusion

it is important to understand CSRB as a body is positioned to do something no one else does - understanding how and why complex digital systems fail and how to mitigate or event prevent such failures in future. Its value is considerably reduced where it duplicates other efforts and activities, such as those focused largely on the behavior of specific threat actors, regardless of how active or meaningful its contributions. The investigation of the failure of complex systems, not for fault but for cause and context, is unique in cybersecurity. To conduct investigations of incidents selected without consideration for the political cost or timing is unique. To complete and publish these investigations without regard for profit motive or repeat business, is unique. These three elements, at least, are unique to what CSRB promises to be – 1) focus on systems and not actors or harms, 2) nearly automatic incident selection, insulated from politics, and 3) publication of results without regard for business impact. All three would be substantially valuable to the cybersecurity community and the safety of the public at large and so merit due consideration as to how best to carry them out.

[38] https://www.ntsb.gov/about/history/pages/default.aspx

[39] https://www.ntsb.gov/news/press-releases/Pages/NR20220510.aspx