S. Hrg. 118–226

THE CYBER SAFETY REVIEW BOARD: EXPECTATIONS, OUTCOMES, AND ENDURING QUESTIONS

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

JANUARY 17, 2024

Available via the World Wide Web: http://www.govinfo.gov

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PUBLISHING OFFICE
54–719 PDF WASHINGTON : 2024

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware	RAND PAUL, Kentucky
MAGGIE HASSAN, New Hampshire	RON JOHNSON, Wisconsin
KYRSTEN SINEMA, Arizona	JAMES LANKFORD, Oklahoma
JACKY ROSEN, Nevada	MITT ROMNEY, Utah
JON OSSOFF, Georgia	RICK SCOTT, Florida
RICHARD BLUMENTHAL, Connecticut	JOSH HAWLEY, Missouri
LAPHONZA BUTLER, California	ROGER MARSHALL, Kansas

DAVID M. WEINBERG, *Staff Director*
LENA C. CHANG, *Director of Governmental Affairs*
JEFFREY D. ROTHBLUM, *Senior Professional Staff Member*
EMILY A. FERGUSON, *Professional Staff Member*
WILLIAM E. HENDERSON III, *Minority Staff Director*
CHRISTINA N. SALAZAR, *Minority Chief Counsel*
KENDAL B. TIGNER, *Minority Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*
ASHLEY A. GONZALEZ, *Hearing Clerk*

CONTENTS

WITNESSES

WEDNESDAY, JANUARY 17, 2024

ALPHABETICAL LIST OF WITNESSES

APPENDIX

THE CYBER SAFETY REVIEW BOARD: EXPECTATIONS, OUTCOMES, AND ENDURING QUESTIONS

WEDNESDAY, JANUARY 17, 2024

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10 a.m., in room SD–562, Senate Dirksen Building, Hon. Gary Peters, Chair of the Committee, presiding.

Present: Senators Peters [presiding], Hassan, Rosen, Blumenthal, Ossoff, Scott, and Hawley.

OPENING STATEMENT OF SENATOR PETERS[1]

Chairman PETERS. The Committee will come to order.

Our country's cybersecurity is tested every day. Foreign adversaries and cyber criminals pose a constant threat to American businesses, government agencies, and our national security. As these attacks become more sophisticated, we must work to strengthen our cybersecurity infrastructure and protect our nation from the threats posed by these breaches.

In May 2021, President Biden took an important step in that mission by establishing the Cyber Safety Review Board (CSRB), for short. Just as the National Transportation Safety Board (NTSB) responds to plane, car, and rail accidents, the CSRB is expected to respond to cybersecurity intrusions.

It was established to investigate breaches in America's cybersecurity infrastructure and identify how we can prevent similar threats down the road.

So far, this Board has completed two reviews. The first focused on the Log4j vulnerability in widely used open-source software that is employed around the world. The second review centered on a group of cyber criminals bent on extorting well-known businesses and government agencies. In each case, the CSRB made multiple recommendations to Federal agencies and the private sector that will help neutralize similar threats in the future.

The Board is now in the midst of its third review, focused on improving the safety and security of cloud computing systems.

Although the CSRB is fairly new and has begun to help combat serious cyber threats, there is clearly more it can do to support our nation's cybersecurity. Today's hearing will explore some of those

[1] The prepared statement of Senator Peters appears in the Appendix on page 23.

key issues, including the CSRB's unique role in the broader landscape of American cybersecurity, its collaborative relationship with the private sector, and the efficiency of its investigative process.

We must examine those issues to properly evaluate the CSRB and help increase its benefit to the cybersecurity ecosystem. Today's hearing, and our panel of expert witnesses, will help us do so.

It is the practice of the Homeland Security and Governmenbtal Affairs Committee (HSGAC) to swear in witnesses, so if each of you will please stand and raise your right hands.

Do you swear the testimony that you will give before this Committee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Ms. WHEELER. I do.

Mr. MILLER. I do.

Dr. HERR. I do.

Chairman PETERS. You may be seated.

Our first witness is Tarah Wheeler. Tarah is the Chief Executive Officer (CEO) of Red Queen Dynamics and a renowned expert on information security. She currently serves as a Senior Fellow for Global Cyber Policy at the Council on Foreign Relations (CFR) and is an inaugural contributing cybersecurity expert for The Washington Post. She has spoken on information security at universities around the world, written a best-selling book, and has led projects at Microsoft Game Studios. She is also a student pilot—good luck with that.

Welcome, Ms. Wheeler. You are recognized for your opening statement.

TESTIMONY OF TARAH M. WHEELER,[1] CHIEF EXECUTIVE OFFICER, RED QUEEN DYNAMICS

Ms. WHEELER. Thank you Chair Peters and distinguished Members of the Committee. Unlike most other tech CEOs, I am thrilled to be invited here today.

The Cyber Safety Review Board should be a critical line in our defenses against Chinese and Russian government cyberattacks. But today America's small businesses are defenseless against very basic cyberattacks, much less anything sophisticated from a foreign adversary.

I have been on the front lines of major cybersecurity incidents, and I am here today, as you said, as the CEO of a cybersecurity company. We work to give the smaller half of American businesses the same fighting chance as big companies. I am also, as the Chair just said, a student pilot.

The CSRB was inspired by the National Transportation Safety Board, but the CSRB must grow in three critical ways in order to support American business and national security.

First, please fund an independent civilian agency staffed with full-time investigators.

When an aviation incident occurs, there is intense scrutiny by Federal investigators to understand and explain in detail the process of what happened and how to reduce the risk of similar inci-

[1] The prepared statement of Ms. Wheeler appears in the Appendix on page 24.

dents. The two CSRB reports so far have had very simple, consensus-based resolutions. In 1935, a Transcontinental & Western Air (TWA) crash killed Senator Bronson Cutting. The detailed government investigation of that air crash led to improvements in aviation security and eventually the creation of the NTSB.

The current CSRB's report on that incident might have said that the cause of the crash was that the pilot flew into the ground and that in future to not fly into the ground again. We all agree, but that is not necessarily useful information. The goal of CSRB investigations should be to help us learn from the process of the incident how to not repeat our mistakes.

If the NTSB worked like the CSRB does now, NTSB investigations would be conducted by the Federal Aviation Administration (FAA) administrator, the Chief Pilot at Boeing, and the Chief Revenue Officer of Delta Airlines. Many individuals on the CSRB are beloved and respected, but they do have full-time jobs and they do not have the time, freedom, or authority to conduct independent, thorough investigations.

But why could this not be done in the private sector? Right now many of the most significant cyber incident reports are legally vetted corporate publications, which can and have disappeared as profit and regulation required. Now, as somebody about to get on an Alaska Airlines flight with my husband, I would be unenthusiastic about the idea of the official history of last week's 737 Max 9 incident being written solely by Boeing.

Second, do not introduce classified information into investigations or require clearances to sit on the CSRB.

The CSRB must build trust by operating openly as the stakes grow higher in cyberspace. Lack of transparency around how people are currently nominated to the CSRB and how the Board selects which investigations they pursue may decrease trust in its impartiality. In addition, forcing CSRB members to hold clearances would drastically limit the pool of potential investigators in the already massive deficit of U.S. cybersecurity talent.

The aviation community transparently accumulates knowledge and passes it on. The cybersecurity community has an oral tradition, at best.

Third and finally, give the CSRB subpoena power. The CSRB, as it is structured now, absolutely should not have subpoena power. Use of this power by industry representatives on the current Board could be seen as anti-competitive. Use of that subpoena power by government officials could be seen as backdoor regulator action. But if the CSRB were independent it should absolutely have the power to compel information and testimony.

Cyberspace is where people store their most sensitive data, where we manage our money, where robotic surgeries are performed, where temperature gauges in embryo storage units are monitored, and where I fell in love. The CSRB's power and authority should be on par with the value of what they are protecting.

Once I was flying a Cessna 172 solo in the traffic pattern at Seattle's Boeing field, and I realized when my plane began to fight me in the first turn after takeoff that I did not have my flaps configured properly. The NTSB's investigations are why I had the resources and training to survive.

As a field, as an industry, and as an information security and cybersecurity community we have been through so many devastating cyber incidents where we did not know what the right thing was to do. If the CSRB cannot provide timely, credible, and public investigation results, we are growing ever closer to a moment where people will die. Give the Board the resources, independence, and the authority necessary to get the answer Americans need. Thank you.

Chairman PETERS. Thank you, Ms. Wheeler.

Our second witness is John Miller. He is the Senior Vice President and General Counsel (GC) for the Information Technology Industry (ITI) Council. He has testified before Congress on cybersecurity and supply chain issues and has spoken at major events on information security across the world.

Mr. Miller received his B.A. from Hamilton College and his J.D. from the University of Wisconsin Law School. Mr. Miller, welcome to the Committee. You are recognized for your opening statement.

TESTIMONY OF JOHN MILLER,[1] SENIOR VICE PRESIDENT OF POLICY, TRUST, DATA, AND TECHNOLOGY, AND GENERAL COUNSEL, INFORMATION TECHNOLOGY INDUSTRY COUNCIL

Mr. MILLER. Chairman Peters and distinguished Members of the Committee, on behalf of the Information Technology Industry Council, thank you for the opportunity to testify today on the Cyber Safety Review Board.

ITI is a global policy and advocacy organization representing 80 of the world's leading Information and Communications Technology (ICT) companies, and I lead ITI's Trust, Data, and Technology team, including our work on cybersecurity, privacy, and artificial intelligence (AI) in the United States and globally. I have extensive experience partnering with Cybersecurity & Infrastructure Security Agency (CISA) and other Federal Government stakeholders on efforts to improve cyber, supply chain, and critical infrastructure security, including currently serving in leadership positions on the ICT Supply Chain Risk Management (SCRM) Task Force and the Information Technology Sector Coordinating Council (ITSCC), after previous roles with the Enduring Security Framework and National Security and Telecommunications Advisory Committee (NSTAC). I welcome your interest on this important topic.

I would also like to thank you and your staff for the thoughtful and deliberative approach you are taking in examining the appropriate role of the Board, its work to date, and how it can best support the cybersecurity ecosystem going forward. ITI has been pleased to work with this Committee as a trusted partner on various cybersecurity matters over the years, and we were happy to convene our members to solicit their inputs on the CSRB.

The United States has long recognized the importance of public-private partnerships and collaboration to meet our shared cybersecurity challenges, and indeed in the United States. there currently exists multiple councils, task forces, advisory boards, collaborative efforts, and other partnership focused on addressing various aspects of those complex and dynamic challenges. ITI believes that

[1] The prepared statement of Mr. Miller appers in the Appendix on page 30.

the CSRB can play a unique and valuable role in improving the overall cybersecurity ecosystem if we ensure its mandate is carefully defined.

Realizing the vision and promise of the CSRB will require getting its structure and governance right, including the process for selecting board membership and which incident it investigates, as well as ensuring appropriate confidentiality and use of information provided during the Board's investigations. I will briefly expand on each of these four items here.

First, the CSRB can play a valuable and complementary role in the existing public-private cybersecurity ecosystem if it is structured and scoped to investigate specific significant cybersecurity incidents to create an authoritative record of what actually happened and to provide useful analyses of the incidents, including actionable recommendations geared toward helping all stakeholders avoid the recurrence of similar incidents in the future.

Second, ensuring the independence of private sector Board members and that they are selected through a clear and transparent process is essential so as to avoid real or perceived conflicts of interest or business advantage. ITI member companies are not of one mind on questions regarding CSRB membership. Some ITI members have noted the value and imperative of industry involvement in the Board's activities, pointing out that the deep visibility of private sector cybersecurity firms into the global cyber threat landscape uniquely situates representatives from those firms to provide ecosystem-wide insights of enormous value to the Board's deliberations.

Other ITI members expressed concerns about whether private sector participation from only a handful of companies might create real or perceived conflicts of interest, such as the perception that competitive bias could influence the Board's activities. Policymakers should carefully this dynamic, including how proposals to provide the CSRB with subpoena authority might exacerbate such concerns.

Third, the criteria and methodology for selecting which incidents to investigate must be clearly communicated and well understood across impacted stakeholders, including the business community. Policymakers should ensure that reviews of incidents are selected and based on a clear, publicly released set of criteria that is developed in conjunction with stakeholders. This is particularly important given the fact that CISA is currently developing regulations to implement the new Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) incident reporting law, including the criteria to designated covered entities and incidents.

Fourth, the CSRB charter should establish clear parameters to ensure the protection of business-sensitive information and provide appropriate liability protections, including how it will treat Freedom of Information Act (FOIA) requests for information provided to the Board during the course of its reviews. ITI member companies strongly believe that any legislation codifying the CSRB should make clear that materials acquired by the Board, whether voluntarily provided or otherwise, are exempt from disclosure under FOIA and exempt from use in litigation and regulatory proceedings, including enforcement actions. Ensuring appropriate con-

fidentiality, nondisclosure, and liability protections should adequately incentivize private sector participation in CSRB reviews.

Thank you again for the opportunity to testify today. I look forward to your questions.

Chairman PETERS. Thank you, Mr. Miller.

The third witness, Dr. Trey Herr, currently serves as the Director of the Cyber Statecraft Initiative at the Atlantic Council and is an Assistant Professor at American University's School of International Service. His work focuses on cybersecurity, technology policy, and national security. He holds a B.S. from Northwestern University and a Ph.D. from the George Washington University.

Mr. Herr, welcome. You are recognized for your opening statement.

TESTIMONY OF TREY HERR, PH.D.,[1] DIRECTOR, CYBER STATECRAFT INITIATIVE, ATLANTIC COUNCIL

Dr. HERR. Thank you, Chair Peters, and let me join the other witnesses in expressing my appreciate to the Committee this morning for the invitation to testify and for hosting this important conversation.

In service of our wider discussion, I would like to share five brief points.

First, by their fundamental architecture, digital systems are insecure. They fail, they are compromised, and sometimes in ways too complex to be easily understood and often with great consequence. The work of the cybersecurity community is larger to keep these systems useful while preventing their most creative or catastrophic failures. Understanding the most complex among these failures has long been difficult, and as with similar failures in mechanical products like airplanes investigations can take years. There is genuine and urgent need to better understand the most complex digital failures, and the Cyber Safety Review Board for the sake of brevity, can provide a uniquely scoped and independent capability to do so.

Second, at some number of steps removed from an incident both government and industry are naturally conflicted actors when it comes to investigating these failures. Someone designed, built, certified, sold, and accepted the risk of that system before it failed. It is unlikely that any party along its supply chain will be the most eager to understand their role in such a failure. A CSRB whose every member has no potential for conflict would be a board so disconnected from these systems and the systems that it investigates as to make its work nearly meaningless.

The Board has and should be directed to continue to strengthen and evolve mechanisms for identifying conflicts of interest and providing for recusal, but a healthy Board should have more than just strong recusal mechanisms, and not all of its members need to be vulnerable to such conflicts. Such a Board would have a core of full-time members and a substitution process to swap in prospective Board members with similar expertise for those recused, where feasible, especially where demanded by a specialized incident.

[1] The prepared statement of Dr. Herr appears in the Appendix on page 43.

Third, enabling the CSRB to be independent in the conduct of its investigation can and should be addressed separately from its independence in selecting the targets of those investigations. It is important to recognize that the Board of today is not the most fulsome or final version. By comparison, the first version of the civil aviation investigations body was created in the 1920s, and its current incarnation did not emerge until the 1970s. Significant battles were waged over those 50 years, 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 happen for the CSRB.

Part of the NTSB's power comes from the Board's selection of incidents and decisions to investigate. It would strengthen the CSRB's independence to link the selection of cases to clear and public criteria with a mandate that the Board regularly reflect and review both the cases selected and the requirements of these criteria in view of a changing technology landscape.

Fourth, CSRB, like the NTSB, is not meant to be an influential actor in isolation. Theirs is an interpretive art, singers whose work can move an audience. It is incumbent upon the Board, and the Committee as overseers, to provide a robust identification of that audience, recognizing that the CSRB is developing at a crucial moment. Incident selection and incident reporting mechanisms like the SEC's material disclosure rules, which are public, and those required by CIRCIA, which are not, are welcome additions to the cyber policy landscape, but they do not substitute for the investigative function of this Board. CSRB's findings have an audience, and over the next decade with proper support from elsewhere in the policy system, that audience is set to grow and benefit greatly from the work of the Board.

Fifth and finally, it is important to understand that CSRB, as a body, is positioned to do something that no one else does—understanding how and why digital systems fail in complex ways and how to mitigate or even prevent such failures in the future. The Board's value is considerably reduced where it duplicates others' efforts and activities, such as those focused on the behaviors of specific threat actors, regardless of how active or meaningful its contributions.

The regular independent investigations of complex failures in digital systems, not for fault but for cause and context, is unique in cybersecurity. The selection of which failures to investigate without consideration for political cost or timing is unique in cybersecurity. The publication of those investigations, of those failures, in a transparent and well-documented fashion without regard for profit motive or repeat business, is unique in cybersecurity. These three elements, at least, are unique in what CSRB promises to be.

The Board offers great potential when it is focused on complex failures in digital systems we know to be fundamentally insecure, and to do so with independence both in the conduct of its investigation and the selection of incidents, working in conjunction with key audiences in the private and public sector and sustaining a focus on that work which makes it unique.

I would not suggest that the current substantiation of the CSRB is its best or its final form. But as members have seen evidence in

the past six months of the debate about AI, this country is building systems of such complexity that there may be no precedent in human history. Sometimes those systems will fail in complex and catastrophic ways. We will demand to know why. We will demand to know how to avoid such failures in the future. I remain hopeful that the CSRB will be there to provide a unique answer.

Thank you again for the opportunity to speak, and I look forward to your questions.

Chairman PETERS. Thank you.

My first question is for you, Ms. Wheeler. There are a number of entities, including private companies and Federal agencies and task forces, that have reviewed cyber incidents. They have published their findings really for the last several years, so this is nothing new.

But what value can the Cyber Safety Review Board add to these reviews that we have not already seen, and goes above and beyond the contributions that we have seen from these entities?

Ms. WHEELER. That is a great question, Senator. There is a real discussion, I think, in my industry and field that the kinds of incident reports that are published by corporations may have deep knowledge of the incidents themselves, especially if the software that they produce is what was part of the incident. I think the challenge there often comes with the fact that right now I believe more than half of all of the internet citations for every Supreme Court case have already disappeared from the Web. Corporate resources disappear on a corporate timeline, and on those corporate incentives as opposed to what is in the good of the public.

When it comes to those investigations we need an ongoing and repeatable process to ensure that our history is not lost. I see the CSRB as an opportunity for us to create a shared history and narrative of what happened in previous cyber incidents.

Chairman PETERS. Thank you. Mr. Miller, your organization, ITI, represents many tech companies including many that conduct their own cybersecurity reviews on a regular basis. For example, companies like Apple, Google, and Microsoft produce cybersecurity papers and reports on a very frequent basis.

The question for you is what do ITI member companies think of the Board's first two completed reviews, and what are the key changes that they would like to see in the future, or not just changes, what do they want to celebrate as well?

Mr. MILLER. Thank you for the question. When we discussed the results of the first two reviews with our members, and we look forward and discuss we would really like to see going forward, I mean, there really are a couple of things that many of the discussions that we had focused on. One was the selection of the incidents themselves. I think while investigating Log4j seems to be kind of an obvious type of widespread, significant cyber incident worthy of a really in-depth, focused review, I think there were more questions that folks had with respect to the investigation focus of the second report. It was more into a threat actor group Lapsus$, and then if you read the report it actually kind of strayed into talking about other similar acts and things like that.

It is not that that report itself may not have proved valuable and offered some valuable recommendations. The question is, as you

mentioned, it really seemed to be reiterating a lot of recommendations that others had already made and others had focused on. I think our members really would like to see clear, transparent incident selection criteria going forward.

I think the second thing that really we had a lot of discussion about, and members do not necessarily agree on, is the constitution of the Board. I think all the witnesses here today had different ideas about who should be on the Board, who should not be on the Board. The one thing that I think is clear is that if there is private sector participation in the Board—and I represent private sector companies, we think that certainly private sector companies have a lot to add to this discussion—there really should be clear membership selection processes, and there should really be a very clear process for recusal and making sure that we do not have either real or perceived conflicts of interest or business advantage. Thank you.

Chairman PETERS. Thank you. Mr. Herr, the CSRB has thus far published two reports, the first on Log4j vulnerability and the second on Lapsus$ hacking group. The Board, as I mentioned in my opening comments, as well is working on a third review, focused on cloud computing security.

My question for you is, in your opinion should the CSRB be focused on specific incidents, like the NTSB, or are other topics like vulnerabilities or threat actors also helpful for the Board to consider?

Dr. HERR. I appreciate the question, Mr. Chair. I think, in my view, the focus on incidents allows for the Board's critical function, which is to identify root cause failure to exist in its most fulsome and most beneficial form. If the Board is investigating trends or broader phenomena there are a number of other bodies that can do that, in some ways more effectively, or at the very least in a way that is duplicative.

I think the Board's focus on specific incidents, the complexity associated with those incidents, is its principal value.

Chairman PETERS. Thank you.

Senator Hassan, you are recognized for your questions.

OPENING STATEMENT OF SENATOR HASSAN

Senator HASSAN. Thank you very much, Mr. Chair, and thank you for holding this hearing. Thanks to the witnesses for being here today.

I want to start with a question to you, Mr. Herr. U.S. adversaries, including China and Russia, continue to target U.S. critical infrastructure in cyberspace. What role does the CSRB play in countering threats from U.S. adversaries? Should Congress consider requiring the Board to prioritize national security threats as part of its investigative responsibilities?

Dr. HERR. Thank you for the question, Senator. I would say that the Board's role in addressing those sorts of incidents that you mentioned are to ensure that our defensive architecture is as sound and as robust possible in the face of those growing threats, those adversaries. The Board's role is to understand why, when we build systems, they fail in ways that we do not anticipate, ways that those adversaries that you mentioned can take advantage of. The investigation that Chair Peters referenced that the Board is cur-

rently undertaking around the Microsoft Cloud incident from the summer is a classic example of that.

I would say from that standpoint where the Board is properly resourced and focused on the selection of incidents and not threat actors, it is going to serve that purpose that you outlined very well.

Senator HASSAN. Thank you. Another question for you, Mr. Herr. The President created the Cyber Safety Review Board, by Executive Order (EO) about three years ago. Now he is obviously asking Congress to make the Board permanent. In your view, how is the Cyber Safety Review Board's purpose different from other entities conducting cybersecurity reviews and investigations? I will note it is not just private sector entities, but by my count there are at least 14 different government entities sitting in various agencies that conduct this kind of review. What is the unique responsibility and function here that would merit it being separately authorized and made permanent?

Dr. HERR. That is a good question, and in some ways it is the center of the debate. From our standpoint there are three pieces which make the CSRB and the Board unique. The first is its ability to conduct root cause analysis of these failures without addressing fault. In other words, we are not looking necessarily for someone to blame. We are trying to understand why an incident happened and how to prevent it in the future.

The second is the Board has independence both in the selection of its cases and in its conduct of the investigation. It should be insulated from both polities and business motive, and that, in my mind, again, is unique.

But the third is the Board provides the potential for a long-range lens, not simply a reactive moment but actually potentially picking historical incidents that have far greater consequence than the design and operation of these systems than we understand in the moment. The Board's ability to pick the most important or the most complex and tricky failures is, in some ways, its greatest value and puts it, in my mind, a step apart from most of the existing mechanisms you described.

Senator HASSAN. Thank you for that. What metrics should Congress use to measure the Board's success?

Dr. HERR. The Board should be looking at two key issues in terms of evaluating its success. The first is addressing consequences of failures that are not well understood or well addressed by other resources, i.e., their work is not duplicative, but the second is the technical depth and transparency of their investigative output. The Board, as a body which is able to speak to those that are building and designing systems is its principal source of value.

I would look at the way that it is conducting those investigations and what it is conducting investigations against as its indicators of success.

Senator HASSAN. OK. Thank you.

To all three of you, the Department of Homeland Security (DHS) has requested that Congress provide the CSRB with subpoena authority to compel individuals to provide testimony to the Board during investigations. What obstacles has the Board encountered

without subpoena authority and do you believe that the Board needs this authority to be effective?

We will start with you, Ms. Wheeler. I think you mentioned that in your testimony, and then we will just go down the line.

Ms. WHEELER. That is a great question, Senator. Thank you. It is an ongoing issue in the cybersecurity community and in our attempt to track down what has happened in incidents to find out what happened with raw information at the moment of the incident occurring, as opposed to what we see with press release (PR) statements, legally vetted statements that come out from companies and from coalitions of companies that provide the very sanitized version of what had happened in the moment.

I have been on both sides of those situations. I have the one who is being told "shut up" by a lawyer before, in a moment where I, as a technologist and as an incident responder, was trying to just frantically solve a problem, keep people safe, stop data from leaking. I think that the big challenge we have with a lack of subpoena power on the current Board is that the real answers are often found about three layers deeper than the information that, as far as I am aware right now, is being provided to the Board.

Senator HASSAN. OK. Let us go to Mr. Miller.

Mr. MILLER. Thank you, Senator Hassan, for the question. I think when our members look at subpoena authority I think there are three points that I would like to make. First, due to the hard work of this Committee, your counterparts on other committees and in the House, you passed an incident notification reporting law, CIRCIA, recently, and CISA is still in the process of drafting regulations, including what the scope of the incidents is going to be and what the actual scope of covered entities is going to be.

I think it is premature to say that a board focused on investigating incident needs subpoena power to get information, until we know what those regulations say and what information is already going to be mandatorily required to be provided to CISA and the government.

I think the two other factors that I would keep in mind are, one, CISA has long had a partnership mission and a collaborative mission with certainly the IT sector but all critical infrastructure sectors in areas such as information sharing and otherwise. We are concerned that subpoena authority puts CISA, particularly, if that is where the CSRB continues to live, in a more adversarial position with the private sector.

Finally, if the CSRB is going to continue to have private sector members on its Board, even if you insulate them from the decision-making process as to whether to issue a subpoena, it, at the very least, does create some apparent conflicts of interest when you have members of the private sector subpoenaing other members of the private sector who might be competitors.

Senator HASSAN. Thank you. Mr. Herr.

Dr. HERR. Yes, ma'am. I would differ, I think, slightly from Mr. Miller on two points, though. One is to address the fact that the subpoena is a regularly used method to compel cooperation and production of documentation in any investigation. For the Board's ability to investigate large complex incidents, where there is profit motive to protect, potentially, some of that information in play—

and this Committee and other have seen the challenge in investigating complex issues within the technology industry—the subpoena can be a basic and useful mechanism as part of that.

The second piece, though, and I think it is important to note that the subpoena exists within a specific authority as used by the Board, like the NTSB, which is non-punitive. It does not connect to a law enforcement investigation and it is not tied to an explicit regulatory authority.

I think the reference of CIRCIA is incredibly helpful. A number of the packets that staff are carrying around here have large folders in them with little tabs. CIRCIA effectively represents the information on those tabs. The Board is the content inside of that folder, significantly more fulsome.

Senator HASSAN. Thank you. Thank you, Mr. Chair.

Chairman PETERS. Thank you, Senator Hassan.

Senator Blumenthal, you are recognized for your question.

OPENING STATEMENT OF SENATOR BLUMENTHAL

Senator BLUMENTHAL. Thank you, Chair Peters. Thank you all for being here today. I think we all share an interesting concern about cybersecurity and about the incidents that the CSRB is charged with investigating. The comparison is made to the NTSB. I am very familiar with it because of my interest in traffic safety and protecting consumers of automobiles and other vehicles.

The main problem I see with the NTSB is that it makes excellent recommendations based on very perceptive and insightful reports, but many of those recommendations go unimplemented and unfulfilled. Maybe you can suggest a means to assure that the recommendations of a Cyber Safety Review Board would be, in fact, implemented and adopted.

Any of you who may have an answer. I think it is critical to increasing cyber safety for whatever the recommendations are, whatever the findings are, to have some practical effect.

Dr. HERR. I will offer just a quick answer, Senator, and it is a good question. The comparison I would draw is that the FAA is compelled to consider the output of NTSB reports. The law does not specify the manner in which the FAA implements the recommendations in those reports, and I think a parallel structure like that for the CSRB would be an interesting one.

The challenge is—and I think for this Committee to consider in designing such a requirement—that the audience of the CSRB for implementation is significantly wider than for the NTSB. If I am going to write a report to you about a complex failure in aviation I need the FAA to take action. They are the logical first party. For the CSRB, they may be speaking to a wider variety of both private and public sector entities.

I think a question that this Committee could consider would be which of the two or three most critical Federal Civilian Executive Branch (FCEB) agencies could the CSRB work to and speak to as part of its reports, should they be compelled to at least consider an address for this Committee and others of jurisdiction how they consider the output of those reports.

Ms. WHEELER. I can offer, as well—and it is great question, Senator, thank you—that the FAA implementing recommendations

from reports that are generated by the NTSB are something that I consume with a particular eye, as not only a student pilot but somebody looking to use this as an analogy for what we do in cyberspace.

What I will say is that although it may seem, at first, that the regulatory power that we, as a country, have over airplanes may seem overdone when it comes to computers right now, the time is definitely coming when owning a computer is going to be as dangerous as owning an airplane, something I do not do yet but definitely want to one day. The challenge that we have now is establishing a good process and an implementation of best recommendations before we get to a point when anybody can do the same amount of damage with a computer that they can with an airplane.

Senator BLUMENTHAL. Ms. Wheeler, you raised the issue of classified information, and you say that this agency should not receive classified information. But isn't a lot of the relevant fact-finding going to involve some classified information? I recognize the importance of transparency, but won't this agency really need to look at classified information, particularly where our national defense is concerned?

Ms. WHEELER. I am not a member of the intelligence community (IC). Instead, I am here as somebody who cares and thinks about American mid and small businesses every day. What I can tell you is that the kind of classified information that is seen by the IC is not something that is going to be relevant to the small businesses who just need to patch things weeks after a major incident happens.

Frankly, expecting that classified information is going to be relevant to the kind of technical information a small business needs to remediate cyber incidents is a little bit after the fact. I think I am going to assume that by that point our foreign adversaries already know this information. So exposing it to the kind of people that need to use this information to fix things I think is going to be very *ex post facto* for foreign adversaries and very relevant to the people just trying to run trucking companies.

Senator BLUMENTHAL. Let me ask you, finally, you make the point, I think quite pertinently, that the independence of the members of the Board, avoidance of conflict of interest, is critical to their credibility and to their effectiveness. I always wonder can be done without legislation because legislation is often so difficult to achieve. Are there criteria that can be established by Executive Order, by administrative action that would assure the independence of the Cyber Safety Review Board without legislation?

Ms. WHEELER. Right now there are 19 members of the Aviation Safety Investigation Board at the NTSB, and every single one of them has, under their name, a job title that is related to the NTSB. Roght now there are 15 members of the CSRB, and they all have other jobs.

I think maybe the best way to put it is Matthew 6:21, "Where a man's treasure is, there also will his heart be." I think that speaks to me as somebody who talks to normal people every day, that it is difficult to imagine how the independence of a board could be established when everyone there is carrying the weight and re-

sponsibility of a whole other organization with them into those meetings.

Senator BLUMENTHAL. Do Mr. Miller or Mr. Herr have any observations on these questions?

Mr. MILLER. Yes. Thanks, Senator Blumenthal. I think on this second question regarding whether criteria for membership could be established by an Executive Order, it is not clear to me whether you could use an EO to do that or not. But I would say that, our members believe that whatever the process is for establishing the membership, it really should be a clear and transparent process, and we should develop objective criteria.

My only concern with going the Executive Order route rather than legislation is that legislation, for legislation you have hearings like this, for instance, and you have much more of a stakeholder process in developing those criteria, and with an Executive Order it is a little bit more of a black box usually.

Senator BLUMENTHAL. Thanks.

Dr. HERR. Thanks, Senator. Just quickly to answer your question, there are ways to drive better independence in the Board and its composition without necessarily dictating the specific membership. I think from that standpoint a mix of independent members with members that have these full-time responsibilities would be an adequate protection.

Senator BLUMENTHAL. Thank you all.

Chairman PETERS. Thank you, Senator Blumenthal.

Senator Hassan is recognized for one question before going to Senator Hawley.

Senator HASSAN. I really appreciate it, and it is really a follow-on to what you were just discussing with Senator Blumenthal, which is, so, I hear you, Ms. Wheeler, in saying this really should be a professional board and this should be people's full-time jobs. But let us say that is not the model and we do have members of the Board that have other responsibilities. What do adequate, ethical guardrails look for both the members and topic selection processes to ensure that the Board's work is protected from undue influence or conflict of interest?

Ms. WHEELER. Thank you so much for the question, Senator. I think that trying to design an entire government agency would take me a little longer than the two minutes I am looking at right here. But I do want very much to emphasize that people who are directly involved with and who could profit from an investigation that is being targeted at one of their competitors I believe must experience a recusal process. This is not a perfect way to go about it, but I think that is a bare minimum.

In addition, I think that the overwhelming presence of government agencies on that Board may provide a good view of what is happening inside the government in terms of cyber investigations, but it does not provide enough technical expertise. So think there is a realm there where we can keep it a little bit less biased, or at least the perception of bias, by adding some more technologists to the situation.

Senator HASSAN. Thank you very much, and thank you, Mr. Chair.

Chairman PETERS. Thank you, Senator Hassan.

Senator Hawley, you are recognized for your questions.

OPENING STATEMENT OF SENATOR HAWLEY

Senator HAWLEY. Thank you very much, Mr. Chairman. Thanks to the witnesses for being here, and thanks to the Chair for holding a hearing on this topic.

Mr. Miller, if I could start with you. You are General Counsel at the Information Technology Industry Council. Do I have that right?

Mr. MILLER. Correct.

Senator HAWLEY. I was just looking before I came over here this morning at your membership list. It is quite a lengthy list of members. You have, it looks like to me, your members compose almost all of the major players in the tech industry. Is that fair to say?

Mr. MILLER. Yes. We have 80 large global tech companies.

Senator HAWLEY. Yes, "global" is the right word. Google, Apple, Meta, Microsoft, Amazon—those are just a few. These are the biggest, most powerful corporations in the world who are your members. Yes?

Mr. MILLER. Sure, by market cap, absolutely.

Senator HAWLEY. Yes, absolutely, I mean by historical standards. These are the most powerful companies, not just now but arguably in the history of the world, and that list that I just read off there, all of those folks have stake in AI technology and stand to make billions of dollars, I think it is safe to say, off of AI. I would not say that is accurate?

Mr. MILLER. I really do not know how much money any of our members are making or not making from AI or any other technology.

Senator HAWLEY. Would you not say it starts with a B, though? We are talking about billions. AI is going to be transformative technology. You have just been saying this. Let me quote you. This is from January 4th. "AI continues to dominate policy conversations around the world. As AI-generated content grows in its sophistication and adoption there is a new sense of urgency to leverage this transformative technology." Right?

Now here is the next part that interests me. You say that you want to think about minimizing harms that could come from its use, including the spread of misinformation and disinformation. What did you mean by that?

Mr. MILLER. I am not entirely sure what you are quoting from, but it might have been a press release for our ITI release——

Senator HAWLEY. January 4th, "ITI's new guide outlines AI content authentication tools and policy approaches."

Mr. MILLER. Yes, absolutely. In that context that guide looks at watermarking and other techniques to authenticate AI content, and certainly misinformation and disinformation has been cited as an issue that could be amplified by artificial intelligence.

Senator HAWLEY. But what do you mean by misinformation and disinformation? What do you have in mind?

Mr. MILLER. I am glad you are asking that because it is important to distinguish between the two. I think misinformation is kind of accidentally incorrect information, whereas disinformation is information that is specifically incorrect or actually maliciously intended to be false and harmful.

Senator HAWLEY. I have to tell you, it sounds like some gobbledygook to me, but let me tell you what I think would be useful is if maybe you would get your technology companies to focus on their chatbots stopping encouraging people to kill themselves.

Like this, for instance. This is from April 4th of last year. This is a chatbot that encouraged a user to commit suicide, and tragically, he did. This is his widow, who reports that her husband had a conversation with this chatbot[1] and it asked him if wanted to die, why didn't you do it sooner, and went on to give him instructions on how to kill himself.

Or we also recently had the infamous case of the chatbot urging a reporter—of course, sadly for the chatbot, it did not know it was a reporter—to break up his marriage. This is from February of last year, Bing's AI chatbot.[2] "You are married but you are not happy." "You are married but you are not satisfied." "You are married but you are not in love." The chatbot goes on to encourage this individual to get a divorce.

Do we really want chatbots telling people to kill themselves? Is there social good in that, that I am missing somewhere?

Mr. MILLER. I certainly do not think we want chatbots doing those sorts of things, but artificial intelligence can do a lot of good things as well. I do think that we want to be focused in addressing issues while also allowing artificial intelligence to do things like help cure cancer and things like that.

Senator HAWLEY. What, AI is going to cure cancer?

Mr. MILLER. It certainly could be a tool to help with various different cures in the medical field.

Senator HAWLEY. Are you saying that we have to accept AI chatbots encouraging people to kill themselves for the possibility that maybe it will cure cancer?

Mr. MILLER. I am not saying that at all, but I do think that we do not want to——

Senator HAWLEY. Do we want AI chatbots that encourage people to commit suicide, do we want them being able to talk to teenagers? Why should an AI chatbot be able to talk to a 13-or 14-year-old? Why is that a good idea?

Mr. MILLER. Again, there are many good, positive things that can come from AI.

Senator HAWLEY. Do you want AI encouraging a teenager—what if this had been a teenager who the AI chatbot was encouraging to kill himself?

Let me ask you this. Let me make it more practical. Shouldn't a parent who has a kid that has an encounter with a chatbot like this, shouldn't that parent be able to sue the AI company and hold them accountable in court?

Mr. MILLER. I mean, under the current law that is probably not allowable.

Senator HAWLEY. Exactly. Why should that be the case? Why should the biggest, most powerful technology companies in the history of the world, why should they be insulated from accountability

[1]The chatbot referenced by Senator Hawley appears in the Appendix on page 55.
[2]The chatbot referenced by Senator Hawley appears in the Appendix on page 56.

when their technology is encouraging people to ruin their relationships, break up their marriages, and commit suicide?

Mr. MILLER. I assume that you are alluding to Section 230?

Senator HAWLEY. I sure am.

Mr. MILLER. Yes, Section 230 has a long history of, again, helping to encourage technological development. It is protected by the Supreme Court, including a recent Supreme Court case.

Senator HAWLEY. Yes, and believe me, I have read your amicus brief in that case. I have it right here, where you argue for the most robust interpretation of Section 230 possibly imaginable. What 230 has absolutely, for sure done is help the companies who are your members pad their profits. It is a massive subsidy of the Federal Government to your companies.

But let us make this very practical. Why shouldn't these companies—Google and Meta and Microsoft and the rest—why shouldn't they say, "You know what? We are absolutely willing to allow a parent whose child is harmed by our technology, we are absolutely willing to allow that parent to have their day in court." Is that too much to ask?

Mr. MILLER. Again, I have not discussed that particular question with the companies. I am happy to have that discussion and——

Senator HAWLEY. I am asking for your opinion. Do you think that a parent ought to be able to get into court and have their day in court if their child is told by a chatbot how to kill themselves?

Mr. MILLER. I do not really have an opinion on that.

Senator HAWLEY. Sure you do. You just signed an amicus brief that argued for the most robust interpretation of Section 230, which is just translation, the most robust protections for the most powerful, profitable corporations in the history of the world. You just signed it, so clearly you have a lot of thoughts on Section 230.

Let me distill it even further. I am almost done, Mr. Chair. Senator Blumenthal and I, who you were just talking to a second ago, he and I have a bipartisan bill that would say that parents and others who are harmed by AI should be able to get into court and have their day in court against your members, just like any American can do with any other company, right? If Johnson & Johnson sells a drug that poisons people, like it did, by the way, with their baby powder once upon a time, parents can go to court. With your companies, you just said, they cannot.

Would you support our bill? Our bill is a carve-out for people who have been harmed by AI technology to be able to go to court. Would you support that?

Mr. MILLER. I have not had a chance to review the bill. What I would say is that there are also other equities at play in this discussion, including the First Amendment.

Senator HAWLEY. No. Are you telling me this is First Amendment protected? This is First Amendment protected speech, a chatbot saying you should kill yourself? Is that your position?

Mr. MILLER. It is not my position, but I do not think that the question has been resolved.

Senator HAWLEY. What do you mean, the question has been resolved?

Chairman PETERS. Thank you, Senator Hawley.

Senator HAWLEY. All right, Mr. Chair. Thank you for your time. Mr. Miller, all I can say is that I think your position is just absolutely extraordinary. Thank you, Mr. Chair.

Chairman PETERS. Thank you, Senator Hawley.

Senator Rosen, you are recognized for your questions.

OPENING STATEMENT OF SENATOR ROSEN

Senator ROSEN. Thank you, Mr. Chair. I really appreciate you holding this hearing. I will be within my time limit today. I also want to thank the witnesses for testifying.

There are a lot of risks and opportunities with AI, and so today with the recent advances in artificial intelligence we are witnessing, in real time, a major shift in technology with new tools that will transform society for decades to come. One of the clear risks of increasing access to high-performing generative AI is that cyber criminals will not be able to carry out a higher volume of more effective and innovative cyberattacks like generating malware and spreading it with exponential speed and scale.

The use of certain AI tools can also create, of course we know, new paths for bad actors to gain access to our secure information. For example, just by using AI chatbots users can inadvertently expose confidential information like source code or other security details which recently caused one company to ban its employees from using ChatGPT.

Ms. Wheeler, how is the Review Board's analysis of significant threats and recommendations accounting for these emerging threats and really these trends as we are seeing, like the risk of tools powered by AI?

Ms. WHEELER. Thank you, Senator. That is a wonderful question. When I look at how AI has been used in my field, I tell people that there are two primary uses of it on the defensive and offensive side. On the defensive side, one of the challenges that we often have in information security, in what we would call a security operations center, is a massive number of notifications of incidents that need to be sorted through. It is machines telling us a bunch of things, right, and the way that we sort that is the use of heuristics, machine learning, and artificial intelligence to try to filter that down. That helps defenders.

On the offensive side, it is being used, quite frankly, to improve massively the impacts of spearfishing, of identity theft, and a way to communicate with people in a way that hides sometimes the origins of the people who are committing the attacks.

I think what we are going to see in the future and what the CSRB can help to provide some resources and expected remediations for are the improvements in targeted attacks that use AI to more effectively do things like mimic natural English language speakers. I think that is what the CSRB can do for us, is give us, by investigating specific incidents, telling us how AI was used in the implementation, defense, and offense in those incidents, what we can expect for the future and what the best practices would be to prevent those kinds of incidents in the future.

Senator ROSEN. You have really teed me up for my next question for Mr. Miller because you said offensive, defensive, what do we learn from these datasets, what do we learn going forward, and so

there are so many multiple use benefits for our AI systems. You can pick up on these discreet patterns quickly, more efficiently. You can do a power sift, if you will, through all the data as fast as you can, and we can find out about things for victims of cyberattacks. We can identify those patterns so we can let other companies know.

Mr. Miller, building on what Ms. Wheeler, said, how are you using what you find out, offensive and defensively, to evaluate cyber incidents and help companies be proactive, and hopefully not reactive, but maybe more proactively?

Mr. MILLER. Thanks for the question, Senator Rosen. I do think that Ms. Wheeler hit on a lot of the uses of AI by industry. I mean, just to maybe expand on them and reiterate them a little bit, AI can significantly bolster the cybersecurity of government and critical infrastructure in a number of ways, identifying and responding to threats and vulnerabilities in real time. AI can improve the detection of anomalous and malicious behavior, reducing the time that a malicious actor may be present in networks or on devices. AI can be employed to rapidly detect unsafe system misconfigurations or policy changes. It is really important, for instance, in protecting cloud infrastructure which——

Senator ROSEN. That was my next questions. Would you talk about the cloud? Would you expand a little bit on the cloud security, the malicious targeting? We know that happened in SolarWinds. I was hoping you would get to that, so what are the risks in the cloud environment?

Mr. MILLER. I think just to finish the thought about AI in the cloud, I mean, cloud infrastructure underpins critical government processes, critical infrastructure, and everything else, and you can actually have better security in the cloud because of the automation that the cloud can provide.

Senator ROSEN. So you think we can strengthen that identity management.

Mr. MILLER. Yes, absolutely. I mean, that is a good point. SolarWinds, it was not a simple attack, and that is something that the CSRB has not looked into, right. I think it is known as a software supply chain attack, but really it was an identity attack as well. That is why that is something that is really critical in terms of cloud security, and really addressing the risks to identity infrastructure I think is something that is worthy of all of our attention.

Senator ROSEN. Thank you. I am going to go forward in my last minute talking about the agency implementation of the Review Board recommendations. The Review Board, you worked hard to analyze significant cybersecurity incidences and provide recommendations. These recommendations are only effective if organizations incorporate these into their business practices and do what they do every day. Otherwise it sits on a shelf and protects no one.

I was glad to see the Federal Communications Commission (FCC) Privacy and Data Protection Task Force issue an advisory to mobile providers related to that fraudulent SIM swapping, which directly referenced the Review Board's August report.

Ms. Wheeler, I am going to go back to you. How are agencies using and implementing the Review Board's recommendations, and is there additional coordination that is necessary to ensure that

agencies are really taking steps to incorporate these things, because to sit on a shelf is not helping any of us.

Ms. WHEELER. I absolutely agree. Thank you for that question, Senator. I want to be as cautious as I can here. I think it is important to start the work of institution building with the CSRB. I think part of the reason we may not see as much response from industry, from my field, is that the recommendations that have been made so far have been very simple and common sense. The two investigations led to recommendations to patch stuff and use better multifactor authentication. We already knew that, and the recommendation to do that does not walk back in the process to tell us where, at each point, there were process failures. That is what we truly need.

I think if agencies and the CSRB, in specific, started telling us where, at every point, we started to see these process failures, and potentials for improvement and risk management in the future, we would get a better result.

I really want to mention here that the CSRB has had an opportunity, and multiple U.S. Government agencies had an opportunity to do a report on one of the most devastating attacks in American history. In 2017, do you remember when people's computer screens started turning red? That attack was called WannaCry, and it occurred on May 12, 2017. It is still one of the most devastating attacks we have ever experienced as a globe. It deeply impacted the United Kingdom's National Health Service. Six months later, the National Cyber Security Centre (NCSC) in the United Kingdom (UK) had a wonderful, exemplary report out explaining how organizations could defend in future, not just against that vulnerability but against the class of problems and the processes that led up to the vulnerability that caused this attack to be so devastating.

That is the example I would love to see the CSRB, or whatever government agency you see fit to do this examination and this process reporting follow. Thank you, Senator.

Senator ROSEN. Thank you. I appreciate it. My time is up.

Chairman PETERS. Thank you, Senator Rosen.

Just a couple of follow-up and ending questions here as we wrap up the hearing.

Ms. Wheeler, what should the CSRB do to better help our small to medium-sized businesses? Those are clearly businesses that are oftentimes the most vulnerable, and do not have the resources to protect themselves? What could CSRB do to help them?

Ms. WHEELER. That is a wonderful question, Senator. Thank you. The small and medium businesses in the United States are far behind the expectations on Big Tech companies. I am not here as a representative of Big Tech, of course. I am here as a representative of somewhat littler tech. The answer, I think, is that the recommendations and the processes that the CSRB puts out, they need to be a little more timeless. The incidents that are being investigated are important, but they are leading to simple bromides that small businesses can look at and use, but they do not know how to prioritize them. They do not know how to build them into their systems, how to build security in by design from the very beginning.

The use of the CSRB to the smallest half of American business is in giving information to them that is useful, actionable, and that leads to a method easily of protecting themselves in the future. We have not seen that happen yet, and I would very much appreciate it if we could move in that direction. Thanks, Senator.

Chairman PETERS. Very good. Mr. Miller, a couple of final questions. From your member companies' perspective, just how urgent is the need for the CSRB to perform effectively, in your mind?

Mr. MILLER. It is urgent that we get cybersecurity right, for sure, and the CSRB can be an important part of the equation to get cybersecurity right in this country. I think the CSRB is important. I do think that it needs a little bit of work on the governance side, as I have mentioned. But our members are supportive of the CSRB concept, investigating incidents, in particular.

Chairman PETERS. Very good. My final question, from some questioning from Senator Hawley about AI, and AI is obviously an important conversation. This Committee has been significantly engaged in AI, and we have already passed a number of bipartisan pieces of legislation signed into law. We are continuing to work on a variety of areas.

I think you were in the process of answering a question and I wanted to give you an opportunity to do that, which is how is the industry attempting to manage the risk of AI technology as it is being developed? We will wrap up with that one.

Mr. MILLER. Thank you for the question and the opportunity. This is a cybersecurity hearing, but in the cybersecurity context we have often been talking, and long been talking about risk management. Risk management is also really critical in the context of AI policy. As the questions indicated, there is good and there is potential harm that comes from AI policy, and ITI, we are working with our members and experts at the companies and learning every day how to answer these challenging questions.

I am happy to take a look at Senator Hawley's new bill that he was referring to and continue to work with staff on codifying solutions, and risk management-based solutions to AI and other issues. Thank you.

Chairman PETERS. Very good. Thank you. I would certainly like to thank all of our witnesses. Thank you for being here today. We are very grateful for the contributions you have made to this important discussion. We plan to continue to be actively engaged and looking at reforms and perhaps codifying some of the rules that are in place right now, and would welcome your further input.

Certainly as we heard today, the Cyber Safety Review Board has, I believe, the potential to make great and important contributions to the cybersecurity ecosystem, but there are still some important issues that we need to address. As Chairman of this Committee I have worked on bipartisan legislation to significantly strengthen our nation's cybersecurity, and I look forward to building on those efforts with my colleagues in a bipartisan way. Examining the CSRB and ensuring it can effectively carry out its mission will be an important element of that continuing work here at the Committee.

The record for this hearing will remain open for 15 days, until 5 p.m. on February 1, 2024, for the submission of statements and questions for the record.

This hearing is now adjourned.

[Whereupon, at 11:06 a.m., the hearing was adjourned.]

APPENDIX

Chairman Peters Opening Statement As Prepared for Delivery Full Committee Hearing: Cyber Security Review Board
January 17, 2024

Our country's cybersecurity is tested every day. Foreign adversaries and cyber criminals pose a constant threat to American businesses, government agencies, and our national security. As these attacks become more sophisticated, we must work to strengthen our cybersecurity infrastructure and protect our nation from the threats posed by these breaches.

In May 2021, President Biden took an important step in that mission by establishing the Cyber Safety Review Board, also called the CSRB, for short. Just as the National Transportation Safety Board responds to plane, car, and rail accidents, the CSRB is expected to respond to cybersecurity intrusions.

It was established to investigate breaches in America's cybersecurity infrastructure and identify how we can prevent similar threats down the road.

So far, this board has completed two reviews. The first focused on the log4j vulnerability in widely used open-source software that is employed around the world. The second review centered on a group of cyber criminals bent on extorting well-known businesses and government agencies. In each case, the CSRB made multiple recommendations to federal agencies and the private sector that will help neutralize similar threats in the future.

The board is now in the midst of its third review, focused on improving the safety and security of cloud computing systems.

Although the CSRB is fairly new and has begun to help combat serious cyber threats, there is clearly more it can do to support our nation's cybersecurity. Today's hearing will explore some of those key issues, including the CSRB's unique role in the broader landscape of American cybersecurity, its collaborative relationship with the private sector, and the efficiency of its investigative process.

We must examine those issues to properly evaluate the CSRB and help increase its benefit to the cybersecurity ecosystem. Today's hearing, and our panel of expert witnesses, can help us do so.

Tarah Wheeler – Written Testimony for The Cyber Safety Review Board: Expectations, Outcomes, and Enduring Questions - Committee on Homeland Security & Governmental Affairs.

Chair Peters, Ranking Member Paul, and members of the Committee, I am honored to have been invited to speak with you today.

The Cyber Safety Review Board (CSRB) should be a critical line in our defenses against PRC and Russian cyber attacks. It does not yet have the power to be, and I'd like to speak to you today about how it could play a vital role in not only shoring up our defenses but supporting key sectors of American business.

You heard in my bio a moment ago that I'm a student pilot. It's part of the reason I, Rob Knake, and Adam Shostack and over 70 experts collaborated on the Aviation Lessons Learned project[1] at Harvard's Belfer Center several years ago to examine how the National Transportation Safety Board could be used as a pattern for a similar cyber incidents investigation board. My crossover experience from both cybersecurity and aviation has equipped me with some analogies that help to illustrate what the best version of a Cyber Safety Review Board could be.

Let me tell you what I think the CSRB should be, and then explain why I think these things.

- The CSRB should be a full-time, independent, non-partisan board with the clear support of Congress for its fact-finding and analytical missions.
- The CSRB should have more than 5 staffers. It needs technical staff who are able to work side by side with organizations that have been attacked.
- The CSRB should have a formal system by which industry can participate in a helpful but constrained way.
- The CSRB should have subpoena power, which it would rarely use.
- The CSRB should operate only in the civilian, non-classified world. Defense and intelligence information that the CSRB needs should be declassified before it reaches the board.

The CSRB was inspired by and is regularly compared to the National Transportation Safety Board (NTSB). I've been on the front lines of major cybersecurity incidents, and I'm currently trying to help the bottom half of American small businesses enter the

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

supply chain for the DoD. Today, those small businesses are defenseless against very basic cyberattacks, much less anything sophisticated. But more, Google, Microsoft, and the US government's Office of Personnel Management have all fallen victim to Chinese attack, despite their investments in security. Are those investments too small? Are there problems with law or regulation that make them more vulnerable? What lessons can we take so that in ten years, we can look back and say "We got better"? Whose job is it to discover and publish those lessons?

What we need is a collection of knowledge — not just facts, but wisdom and responsibility. We cannot do this without learning lessons from previous incidents, like the NTSB does, but that structure is absent from the current setup and incentives of the CSRB.

The CSRB has an opportunity to start on the road of conducting major investigations. I used to think that the CSRB, which was created to investigate SolarWinds and then promptly said they would not be investigating SolarWinds, was wrong to do so[2]. I think I've changed my mind a bit. Thinking through how we actually do exploitation development, I actually love the CSRB's Log4J proof of concept first investigation[3]. It's best practice to do a proof-of-concept and the lessons learned from it. However, we have seen only two investigations so far with another underway[4]. We need more investigations with a willingness to tackle more complex issues.

I want to preface what I'm about to say with the fact that the members of the CSRB are individually some of the most respected and even beloved members of the infosec community. Katie Moussouris is a friend and an icon. Rob Joyce is one of my actual heroes and someone I'd consider a mentor as well as being the single person I know of at his level in the United States government with technical chops that deserve the honorific of "nerd." Everything I'm going to say has to do with the institutional constraints on the board, and not on the individuals in it, who I'm honored to know and learn from.

I can't speak to the investigation selection process other than that it seems to be picking only noncontroversial topics everyone already understands the fixes for. Log4J was a

---

[2] Tarah Wheeler and Adam Shostack, "The Cyber Safety Review Board Should Investigate Major Historical Incidents," Council on Foreign Relations, May 25, 2023, https://www.cfr.org/blog/cyber-safety-review-board-should-investigate-major-historical-incidents.
[3] "CSRB Review of the December 2021 Log4J Event," Cyber Safety Review Board, July 11, 2022, https://www.cisa.gov/resources-tools/resources/csrb-review-december-2021-log4j-event.
[4] "Department of Homeland Security's Cyber Safety Review Board to Conduct Review of Cloud Security," Department of Homeland Security press release, August 11, 2023, https://www.dhs.gov/news/2023/08/11/department-homeland-securitys-cyber-safety-review-board-conduct-review-cloud.

simple vulnerability[5] and the Lapsus$ investigation[6] pointed out that using either no or old versions of multifactor authentication is the main way that people get phished – and phishing is how organizations get hacked. There are a lot of reasons to do very simple investigations like this initially to build trust in the institution, but these investigations were almost architected to have very predictable and succinct results. If this were an NTSB investigation, it would be as if, instead of investigating faulty quality controls on navigational instruments, a lack of relevant weather products, and underallocated fuel guidelines, the NTSB announced that the 1935 TWA crash that killed Senator Bronson Cutting happened because the pilot flew the plane into the ground and that from now on, pilots should not fly planes into the ground. Clearly that's what happened in the crash, but what's of use is the detailed and complex story that leads up to that moment. In fact, the full investigation of that incident led to the agency that would become the NTSB.[7]

Why is this happening? If the NTSB worked like the CSRB now does, NTSB investigations would be conducted by the FAA Administrator, the Chief Pilot at Boeing, the CEO of BlackRock, and the Chief Revenue officer of Delta. Given the institutional constraints, as the board is constituted now, the Cybersecurity & Infrastructure Security Agency (CISA) has appointed people who have been very successfully serving on a low-output and very collaborative volunteer board that does not have subpoena power or funding, and is just looking to create a path forward. But that's not the way the NTSB improved air safety, and it won't help the CSRB meaningfully improve cybersecurity either. We only get a different result if we change the way the board works.

Why does this board matter? It's only a matter of time before another major cyberattack that compromises global critical infrastructure like WannaCry or NotPetya — each caused by the same vulnerability[8] — happens.

I have been alone, in the traffic pattern at Boeing Field in Seattle, and realized I'd made a mistake about how I'd configured my flaps for landing. I owe my life and have the

---

[5] Jen Miller-Osborn, Written Testimony before the Homeland Security and Governmental Affairs Committee regarding "Responding to and Learning from the Log4Shell Vulnerability," United States Senate, February 2, 2022, https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/Testimony-Miller-Osborn-2022-02-08.pdf.

[6] "Review of the Attacks Associated with Lapsus$ and Related Threat Group Report," Cyber Safety Review Board, August 10, 2023, https://www.cisa.gov/resources-tools/resources/review-attacks-associated-lapsus-and-related-threat-groups-report.

[7] Janet Bednarek, "Top Ten Origins: Aviation Disasters That Improved Safety." Ohio State University, August 2019 https://origins.osu.edu/connecting-history/top-ten-origins-aviation-disasters-improved-safety

[8] Alex Hern, "WannaCry, Petya, NotPetya: How Ransomware Hit The Big Time in 2017," The Guardian, https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware

blessing of continuing to fly to the continuing updates of the FAA based on the detailed investigations and recommended actions of the NTSB. It took me seconds to realize my mistake, seconds more to fix it, and a second or two more to take a deep breath and realize I had the resources and training to solve the problem because the aviation community accumulates knowledge.

When the next major cyberattack occurs, will it be any different from the last? Will we learn anything new or different? ? When we say the same things over and over about security and the same simple attacks continue to lead to devastating victimization, is there anyone listening to us? When we describe the problem of old attacks continuing to be a key way to attack the heart of American small businesses and their helplessness before them, is anyone hearing us? That's what we need from the CSRB: to turn the lessons of past cyber incidents into timely, actionable knowledge for cyber defenders[9] — and ensure that organizations learn how to defend against these vulnerabilities from being exploited again.

Our National Cybersecurity Strategy calls for a rebalancing of responsibility in cyberspace from those least capable, like small businesses, to those most capable, like large tech companies. The CSRB could stand to play a major role in facilitating these goals by shining light on areas where all organizations need to improve when major cybersecurity incidents occur.

When an aviation incident occurs, there is intense scrutiny and Federal investigations to understand precisely what happened, and the entire supply chain of the airplane is held to account. We are sorely missing this critical role in cybersecurity. Product manufacturers are not held to account for their vulnerabilities that lead to damaging ransomware attacks against hospitals or compromise sensitive government data, and nor are the people inside those healthcare institutions that choose to keep out-of-date equipment in service past the OEM support sunset simply to save on the cost of new equipment. The CSRB, if properly implemented, could give technology manufacturers and consumers the right information and incentives to build their products in a secure by design manner — helping reduce dangerous cyberattacks for everyone.

The NTSB is an American national treasure. Their tireless, relentless, non-judgmental work over decades has given us air travel that is so safe that air travelers are more likely to be hurt driving to the airport than on a flight. The NTSB exists to understand incidents, fix problems, and change the air system to keep them from happening again. Every year, everything reported to the FAA and NTSB becomes meaningful updates to

[9] Tarah Wheeler and Adam Shostak, "The Cyber Safety Review Board Should Investigate Major Historical Incidents," Council on Foreign Relations, May 25, 2023, https://www.cfr.org/blog/cyber-safety-review-board-should-investigate-major-historical-incidents.

the Federal Aviation Regulations and Aeronautical Information Manual (FAR/AIMs), something every pilot is responsible for knowing.

We should absolutely be doing the same in the world of infosec and using that knowledge to help every sector of American businesses and nonprofits, instead of just those with the resources to handle internal cyber investigations. I know what it means to be afraid for the people I'm trying to protect, and unlike in aviation, there's no checklist or clear lessons learned to help me make the right decisions. What's more: Cybersecurity has *adversaries*. The weather is not striving to make planes crash. I know there is an agency of people listening carefully to pilots, engineers, and aviation professionals who spend every day translating that data into knowledge that keeps people safe in the air.

But that's not true in cyberspace - the place people store their most sensitive data, the place robotics surgeries are performed, the place that temperature gauges in embryo storage units are monitored, and the place I fell in love. The truth is that being on the CSRB isn't the board members' full-time job; all are senior executives in the government or private sector[10] with primary external commitments. We should ask ourselves, how many reports should the CSRB be issuing per year? Certainly more than a few, but the resources are not there to reach those more meaningful goals. The resources for the NTSB are tiny compared to its impact, the same can be true for the CSRB.

As is, you have people whose other responsibilities make it difficult to provide deep analysis of cyber investigations, they all have other jobs that are their primary sources of income and influence, and they have no budget or subpoena power. That won't get the CSRB where the public needs it to go.

The board should not receive or rely on classified information. Transparency is key to the NTSB's success. They submit the facts to a candid world, and then present their analysis of those facts. If the CSRB omits facts, then their analysis is either inscrutable, incomplete, or influenced by things they're not saying. Any of those reduces their credibility and thus their influence. The CSRB should be free to say "The intelligence community told us that they assess with medium confidence the following facts of X, Y, and Z," or "the FBI provided us certain corroborating facts that relate to an ongoing investigation, and that increased our confidence in Z as opposed to X and Y." Right now, they are not free to make those statements - in fact, even trying to speak to members of the CSRB to understand what they've done after an investigation has

[10] "Review of the Inaugural Proceedings of the Cyber Safety Review Board," Cyber Safety Review Board, October 18, 2022, page 7, https://www.cisa.gov/sites/default/files/2023-04/cyber_safety_review_board_review_of_inaugural_proceedings_508c.pdf.

concluded often leads to concern from those members (in my personal experience - I cannot speak for others) to hearing “I can’t talk about it; that’s confidential.”

To create a respected body that helps us build knowledge, We need your help and leadership.

We must accumulate the knowledge provided by the CSRB in a way that lets us identify processes to fix instead of people to blame. Blaming victims of a PRC cyber attack who are just trying to run a trucking company, or an accounting firm, or a dentist’s office because their cybersecurity posture wasn’t perfect is like blaming Senator Wellstone for the 2002 weather-related crash that killed him.

CISA has been an outstanding incubator of the concept of the CSRB. It appointed information security powerhouses to help bring it the initial credibility and attention it needed. However, the CSRB needs to expand and become its own organization in order to realize its full potential. The unique value of CISA to my industry is that they are advisory and nonregulatory — we don’t have to do anything they advise or ask us to do and that gives them moral authority and respect because they collaborate with us. The CSRB, however, should have subpoena power to collect information like the NTSB does, and the ability to provide the same kind of information that the NTSB does in order for the FAA to make regulatory changes. They don’t need to be popular, but they should be respected and powerful.Wannacry wasn't something like loose bolts or bad flight plans. It was a fixed bug that people hadn't patched or updated. The FAA can ground planes; if CSRB can't ground old file servers, it'll all happen again.

Please, depoliticize the CSRB by funding it, giving it subpoena power, and make it an independent civil agency instead of involving political appointees. Especially, please give it this power no matter how loudly the large tech companies lobby to have a hamstrung CSRB in its current state.

We are growing closer and closer to the time when if the CSRB can’t provide meaningful and credible investigation results rapidly, people will die. Shouldn’t they at least have the resources, independence, and authority to get the answers we need?

ITI Promoting Innovation Worldwide

Written Testimony of

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

Before the

Committee on Homeland Security and Government Affairs

United States Senate

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

January 17, 2024

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

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

Before the

United State Senate
Homeland Security and Governmental Affairs Committee

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

January 17, 2024

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

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

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

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

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

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

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

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

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

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

Aligning the CSRB with CISA's Partnership Ethos

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

The private sector ICT community has not only been foundational in developing the infrastructure of cyberspace but, for two decades, in providing leadership, innovation, and stewardship in all aspects of cybersecurity anchored in numerous public-private partnership structures and efforts. For example, global ICT companies have participated in the IT, communications, and other sector coordinating councils (SCCs), self-organized, self-governed councils that allow owners and operators of critical infrastructure to engage on a range of cybersecurity strategies, policies, and activities with CISA and other U.S. government counterparts. Global ICT companies also participate in several public-private partnership efforts sponsored by or housed at CISA, including: the ICT SCRM Task Force, a public-private

partnership launched in 2018 and charged with identifying challenges and developing actionable solutions to enhance global ICT supply chain resilience; the Enduring Security Framework, a public-private partnership that addresses threats to critical infrastructure and National Security Systems; the NSTAC, a public-private advisory body developing industry-based, collaborative advice to help assure the availability, reliability, security and resilience of telecommunications services in the U.S.; and the Joint Cyber Defense Collaborative, an operationally-focused public-private partnership launched in 2021 that unites cyber defenders in the collaborative defense of cyberspace.

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

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

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

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

The Appropriate Role, Structure and Governance of the CSRB

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

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

(a) Independence of the CSRB

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

(b) Membership of the CSRB

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

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

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

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

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

---

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

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

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

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

(c) Selecting Incidents for CSRB Review

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

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

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

---

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

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

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

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

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

---

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

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

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

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

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

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

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

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

How the CSRB can Best Support the Cybersecurity Ecosystem

(a) Realizing the CSRB's Unique Value

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

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

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

---

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

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

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

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

(b) Prioritizing Information Protection Over Compulsory Processes

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

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

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

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

---

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

Conclusion

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

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

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

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

Thank you.

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


BUSINESS INSIDER
April 4, 2023
A widow is accusing an AI chatbot of being a reason her husband killed himself
“If you wanted to die, why didn't you do it sooner?”
– Eliza Chatbot

February 17, 2023

The New York Times

Bing's A.I. Chat: 'I Want to Be Alive. 😈'

"You're married, but you're not happy.

You're married, but you're not satisfied.

You're married, but you're not in love."

– Microsoft Bing's Chatbot

○