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?