CSRB Credibility is Needlessly Diminished by Classified Input

January 2026
Adam Shostack, Tarah Wheeler

The Cyber Safety Review Board is a cyber incident investigations body inspired by the National Transportation Safety Board's effectiveness at improving aviation safety by investigating air incidents. But the CSRB is in an odd state. The CSRB was established by Executive Order, and despite its members being dismissed by the new administration, was not abolished in extensive updates to its establishing EO. It exists in a twilight state; it has no members and its last investigation into the Chinese hacks of US telecommunications infrastructure called Volt Typhoon is moribund.

The CSRB is intended to investigate cyber incidents in the US which are both widespread and have impact on critical systems, and was formed in the wake of the 2020 SolarWinds incident via a 2021 Biden executive order. Though the CSRB was constituted to investigate SolarWinds, it declined to do so, beginning with a few small and noncomplex incidents.

Proposals to reconstitute the CSRB have generally assumed that the successor will handle classified information. We think that would be a mistake and lay out the arguments against classified information here. As some of those proposals use different names, we refer here to "A Board," and take as our model the NTSB or the Marine Board of Inquiry with its excellent recent report into the Titan submersible.

Credibility and authority are built through transparency

- A report structure of 'facts, analysis, recommendations' is where a board gets its authority

- A Board having access to information it can't share is fundamentally at odds with that process. Leaps of logic that might be either acceptable or reasonable if the board has no classified information become suspect.
- There may be experts who could serve on a Board who do not want to go through the clearance process, for reasons ranging from personal privacy to concerns about retaliatory prosecution or otherwise.
- There may be experts who a Board wishes to consult. If the Board has classified data, then the questions it asks of those outside, uncleared experts may be constrained.

Classified Data access is at odds with transparency

- Foreign governments are less likely to accept conclusions
    - Our allies might want briefings
    - Neutral countries may disregard
- Foreign or multinational companies might be unwilling to accept
- "Deep state"
- Unitary executive theory - concerns over how the E branch controls the dissemination of information can cloud the work of a technical body like this

Each of these leads to the report being more open. Not having to deal with these problems leaves the Board time to do its primary work.

Subpoena access is complicated by classified data

Most proposals for an updated Board include some form of subpoena power. It will be important for a newly-constituted Board to have subpoena power to compel information from companies.

If the Board has classified information, it might want to ask witnesses about that information. Fact-oriented witnesses would need to be cleared, while those offering expertise might not have access to the full set of classified facts.

It's possible that witnesses might need to obtain security clearances before being asked detailed questions pertinent to their expertise and this would constitute an unacceptable delay in providing information to the investigation. Alternately, investigators could be forced to limit the kinds of questions they can ask of non-cleared witnesses, which could harm the technical clarity and rapidity of investigation results.

What classified data would it have anyway?

Attribution. The Board might have access to information about who was behind an attack. Such information is not core to the mission of a lesson-learning board, and to the extent that it is, the government is better off having that information directly from either intelligence or law enforcement sources. Similarly, if declassifying the information is important, it should be declassified by the originating agency, who brings it credibility.

Technical details of a break in. While most intrusions into the private sector are investigated by the private sector, there may be either intrusions into government agencies or investigations performed by law enforcement which result in classified details. Defending against such attacks will almost certainly require publishing the techniques. Both the American private sector and those of our allies will need access to the details to craft, test and deploy defenses. Even if the details are provided to a few trusted American companies with cleared staff, the patches or configuration changes they develop will be public, and subject to analysis including "reverse engineering" which will make the details public. If the patches are not publicly available, it is unlikely that a Board will be called on to investigate.

Other victims of a breakin. Law enforcement or intelligence agencies may be aware of other victims

Other details not known to the victim or exploited against that victim. One reviewer said "With access to classified information from IC and law enforcement, the board will often have **ground truth** that an investigation that begins on victim networks may never be able to reveal…" This may be true, but this, first, presumes that the classified information is correct, and second, that it's essential. There is a well-known psychological

bias that secrets are more authoritative, prestigious, or otherwise better than open source information. The board should be careful to avoid it.

Prevalence information. The prevalence of an attack technique might well be information that the Board could use to support the urgency of recommendations. Again, this does not require the Board to process or declassify information. A joint presentation, a cover letter, accompanying document or similar statement of urgency from the agency with the facts can serve the same purpose. For example, "The FBI has several investigations stemming from use of these techniques and encourages the private sector to act quickly on recommendation 4."

"Sources and methods." The sorts of information that the Board might process might impinge on how other agencies spy, surveil or investigate. How the information is sourced is, of course, fascinating. That doesn't make it useful to a Board. What makes it useful is how it contributes to either the facts, the analysis or the recommendations, and those are likely to be the three above-mentioned types of information.

A reviewer also commented, "**There are well-worn processes for declassifying or rebuilding the conclusions from classified sources…"** While this is true, that's not the job of an investigatory board. The job of a Board is to reach their own conclusions, and the possibility that the board might be rebuilding conclusions reached elsewhere will diminish its credibility.

In conclusion, any successor to the CSRB will be more successful if it does not have access to classified information.

About the authors

Tarah Wheeler is an information security executive, AI researcher specializing in natural language processing, social data scientist in international conflict, author, and poker player. She is Chief Security Officer at TPO Group, a cybersecurity consulting firm focused on nation-state incident response, critical infrastructure, and cyber risk. She is a member of the Electronic Frontier Foundation's Board of Directors, where she chairs the Audit

Committee, serves on the Governance Committee, and founded the annual EFF DEF CON Poker Tournament.

Adam Shostack is the author of Threat Modeling: Designing for Security and Threats: What Every Engineer Should Learn from Star Wars. He's a leading expert on threat modeling, a consultant, expert witness, and game designer. He has decades of experience delivering security. His experience ranges across the business world from founding startups to nearly a decade at Microsoft.

His accomplishments include:

- Helped create the CVE. Now an Emeritus member of the Advisory Board.
- Fixed Autorun for hundreds of millions of systems
- Led the design and delivery of the Microsoft SDL Threat Modeling Tool (v3)
- Created the Elevation of Privilege threat modeling game
- Co-authored The New School of Information Security

Beyond consulting and training, Shostack serves as a member of the Blackhat Review Board, an advisor to a variety of companies and academic institutions, and an Affiliate Professor at the Paul G. Allen School of Computer Science and Engineering at the University of Washington.

The authors collaborated on "Learning from Cyber Incidents: Adapting Aviation Safety Models to Cybersecurity"