CYBER SAFETY REVIEW BOARD

CYBER SAFETY REVIEW BOARD: FAQS

The Cyber Safety Review Board (CSRB) conducts reviews of significant cybersecurity incidents so that government, industry, and the broader security community can better protect our nation's networks and infrastructure. After conducting fact-finding, the Board issues actionable recommendations based on the lessons learned from each incident.

What is the Board's composition?

The Secretary of Homeland Security (DHS Secretary) has delegated to the CISA Director the responsibility assigned in Executive Order 14028, *Improving the Nation's Cybersecurity*, to appoint standing members of the CSRB. The Board's membership includes the federal government's leads for cybersecurity, from across agencies, and cybersecurity luminaries who work in the private sector. In order to fully leverage broad-ranging experience and education, the Board must be diverse with regard to professional and technical expertise. To be eligible to serve on CSRB, members and subcommittee members must be U.S. citizens and be able to obtain a security clearance. Private sector members serve as Special Government Employees (SGEs) and are subject to Federal ethics requirements, including compliance with financial disclosure programs and annual ethics training. The private sector members serve in their personal capacity, and, as such, are expected to bring independent expertise to the CSRB rather than reflecting or representing the equities of any current or previous employer.

What are the selection criteria for which incidents the Board reviews?

Per Executive Order 14028, the DHS Secretary shall convene the Board following a significant cyber incident triggering the establishment of a Cyber Unified Coordination Group (UCG), as described in PPD-41, at any time as directed by the President; or at any time the DHS Secretary deems necessary. In October 2021, the DHS Secretary delegated this tasking authority to the Director of the Cybersecurity and Infrastructure Security Agency (CISA Director). Unless an incident triggers the establishment of a UCG, only the President, DHS Secretary, or CISA Director have the authority to task CSRB to review a cyber incident or event, as they deem necessary.

Factors that the DHS Secretary and CISA Director consider when deciding what matters to task for the Board's review include:

- The severity and impact of an incident;
- The degree to which the incident exposed weaknesses in the broader cybersecurity ecosystem, such that there are likely to be significant and new lessons learned that will enable the broader community to elevate its security;
- The degree to which the Board can shed new light on an incident and its lessons learned, taking into account whether others have already analyzed the incident at length in the public arena;
- Whether a review will likely lead to a better understanding of issues that will tangibly drive better security outcomes in this country; and,
- Any other factor that would make a review in the public and national interest.

What are the ethics rules that govern the Board, including recusals, to ensure there are no conflicts of interest?

All CSRB members are required to adhere to federal laws establishing ethics standards for federal employees. This includes private sector members, who are serving in their personal capacities as SGEs. All members are required to submit extensive financial disclosure reports and must report any potential conflicts of interest. For reviews in which a CSRB member may have a potentially conflicting interest—such as reviews that involve examinations of their employers' products or those of competitors, or reviews where members have financial interests relating to matters under consideration—the member will be recused from participating in that specific review. For members who recuse or are

excepted from participating in certain areas of a review where a conflict of interest arises, procedures are in place to ensure the integrity of the CSRB's formal findings and recommendations. All ethics determinations are reviewed and approved by career DHS ethics counsel.

For example, in advance of the Board's review of the 2023 Microsoft Exchange Online incident, DHS assessed committee membership and ultimately recused four members from the review. In all, twelve members are participating in the Microsoft Exchange Online review, following a determination by DHS ethics counsel that no conflict of interest or other ethics impediment exist for those members. These twelve members – an experienced group of private and public sector cybersecurity leaders – are driving a thorough review and have all needed resources at their disposal to conduct this important work.

Which matters has the Board reviewed to date and why?

In February 2022, the CISA Director, in consultation with the White House and DHS Secretary, tasked CSRB to review the vulnerabilities discovered in late 2021 in the widely used Log4j software library. These vulnerabilities presented an urgent challenge to network defenders and remain one of the most serious vulnerabilities discovered in recent years. Despite the initial expectation that the inaugural review would address a different incident, the White House and DHS determined that focusing on this vulnerability and its associated remediation process was the most important first use of CSRB's expertise. As recently as December 2023, Cloudflare reported that Log4j remained a top target for attacks in 2023, validating CSRB's finding that the vulnerability would be endemic.

In December 2022, the CISA Director announced that CSRB's second review would be into the attacks associated with Lapsus$, a global extortion-focused hacker group that perpetrated damaging intrusions against multiple critical infrastructure sectors, including healthcare, government facilities, and critical manufacturing. The range of victims and diversity of tactics used demanded an understanding of how Lapsus$ actors executed their malicious cyber activities so as to mitigate risk to potential future victims. In November 2023, the Federal Communication Commission (FCC) adopted rules protecting consumers from SIM swap attacks, with Chairwoman Rosenworcel noting that FCC was adopting CSRB's recommendation that FCC "take action to support consumer privacy and cut off these scams." The timeliness of CSRB's findings and recommendations was further reinforced by the September 2023 attacks on Caesars and MGM that leveraged similar techniques.

In August 2023, the CISA Director tasked CSRB with its third review into the Microsoft Exchange Online intrusion publicized in July 2023, including the malicious access and use of cloud-based identity and authentication infrastructure. As cloud security is the backbone of some of the Nation's most critical systems, and organizations of all kinds are increasingly reliant on cloud computing to deliver services to the American people, it is imperative to understand the vulnerabilities of this technology and how they were exploited in this incident. The CSRB's review of the Microsoft Exchange Online incident is ongoing.

During the course of CSRB's first two substantive reviews, individuals representing approximately 100 unique organizations engaged with the Board and provided valuable information to inform its findings and recommendations. To date, CSRB has engaged with victim companies, academic institutions, threat intelligence firms, incident response firms, security researchers, international law enforcement and cybersecurity agencies, U.S. government agencies, foreign government representatives, critical infrastructure owners and operators, and industry associations, among others.

Does the CSRB have subpoena authority?

No. Under its current organization and authorities, the CSRB relies on voluntary cooperation from the organizations that have relevant information about the events under the review. The Administration has endorsed legislation that would give the CSRB additional authorities, including a limited subpoena authority for information that the Board is not able to obtain through voluntary cooperation. Under this proposed legislation only federal members – and not private sector members under any circumstances – would be permitted to vote on issuance of a subpoena.