Review of the Inaugural Proceedings of the Cyber Safety Review Board

CYBER SAFETY
REVIEW BOARD

October 18, 2022

Table of Contents

1. MESSAGE FROM THE CHAIR AND DEPUTY CHAIR

Pursuant to President Biden's Executive Order (EO) 14028, Improving the Nation's Cybersecurity, we, as the Cyber Safety Review Board (CSRB or the Board), are required to provide the President recommendations with respect to the Board's operations and efficacy based on the Board's inaugural review of the Log4j event.

We believe our review of the Log4j event was a successful proof of concept for this Board. In a short time, the Board reviewed one of the most significant cyber events in history, made significant factual findings that were previously unknown to the community, and issued actionable recommendations that will drive change to elevate our national cybersecurity.

Our focus in this report is to consider the lessons learned from our first review so that the Board will be positioned to build on our initial success through investment in a sustainable, replicable, and professional model for after-action review of the most significant cyber incidents.

We share here our observations and recommendations for this Board's growth and maturation. Our objective is a Cyber Safety Review Board supported by the structure, authorities, and resourcing that will ensure it is built to last as an enduring feature of the cybersecurity ecosystem.

2. EXECUTIVE SUMMARY

The CSRB conducted its first review, of the Log4j software vulnerability event, between February 2022 and July 2022. The CSRB followed a non-Federal Advisory Committee Act (FACA) advisory committee model, was resourced and staffed through existing CISA capabilities, and relied on voluntary participation by potential interviewees. The CSRB met regularly as a full Board, and subcommittees supported its work by exploring specific lines of inquiry. The Board obtained data from public and private organizations through formal requests for information (RFIs), including live interviews with industry experts. The Board leveraged this information to compile its findings and recommendations.

The CSRB took care to create and implement governance procedures to support the Board's work, to include procedures concerning data handling, information protection, conflicts of interest, and other legal and ethical matters. Board staff documented this guidance throughout the process and shared it with stakeholders as appropriate.

Many of the processes and approaches piloted during this review were effective. The Board generally enjoyed a high level of cooperation from industry stakeholders and received responses from over 80 companies. However, some organizations from which the Board requested information declined to cooperate and provide the requested information, in whole or in part. As is to be expected for the initial operational experience of a new organization, the Board did experience some operational challenges that could be addressed and mitigated by the actions and recommendations described below. The Board assesses that these challenges are simply issues the Board must work through as part of the natural maturation process for a new organization; none substantially impaired the Board's ability to achieve its mission of a thorough, independent, and impactful first review.

The Board recommends that Congress codify enhancements to the Board's authorities, to include granting limited subpoena authority to the Board. The Board would also like to work with Congress to begin steady and predictable appropriations to mature the organization, build a permanent staff, and have budget certainty; CSRB staff, based on Board feedback, are developing a proposed budget in parallel with this document to account for these evolving needs.

3. RECOMMENDATIONS

The Executive Order requires the Board to provide recommendations in this report across the following eight categories:

i. identified gaps in, and options for, the Board's composition or authorities;

ii. the Board's proposed mission, scope, and responsibilities;

iii. membership eligibility criteria for private sector representatives;

iv. Board governance structure, including interaction with the executive branch and the Executive Office of the President;

v. thresholds and criteria for the types of cyber incidents to be evaluated;

vi. sources of information that should be made available to the Board, consistent with applicable law and policy;

vii. an approach for protecting the information provided to the Board and securing the cooperation of affected United States individuals and entities for the Board's review of incidents; and

viii. administrative and budgetary considerations required for the operation of the Board.

3.1 Composition and Authorities

EO 14028: "(i) identified gaps in, and options for, the Board's composition or authorities"

Recommendation: No change to the composition of the Board is needed, but the Charter should be modified to reflect the current composition and explicitly include representation from the Office of the National Cyber Director (ONCD).

The Board believes that the number of permanent members is appropriate and conducive to building consensus, while also representing a broad range of views. During the first review, the Board found that 15 permanent members struck the correct balance between broad representation and operational agility. However, the Board also believes that the Charter should be modified to reflect the current members and explicitly note a representative from the ONCD as a Board member.

Recommendation: Congress should enact legislation that codifies the Board, authorizes it to offer confidentiality and other information handling protections and activities, and authorizes limited subpoena authority to obtain necessary information.

Codification of the Board would ensure its position as an enduring independent organization within the cybersecurity ecosystem. This would also facilitate routine and reliable appropriations.

The Board enjoyed a substantial, but not complete, level of voluntary participation during its initial review. The Board's ability to conduct an after-action review will hinge on its ability to obtain relevant information and data from affected parties. Just as aviation accident investigators would require data from a crash scene to undertake their work, the Board will require data to conduct its after-action reviews of cybersecurity incidents.

The Board will require a mechanism to compel involvement, if necessary, although the expectation is this authority would be rarely exercised. In retrospect, Log4j was an "easy" review from the perspective of gaining industry cooperation; it 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. Under these circumstances, many organizations were pleased to cooperate with the Board's review. However, not all did. The Board is mindful that it may be difficult to secure cooperation in some future reviews, for example those focused on an incident that targeted a particular organization that may have incentive not to share what it knows with those outside the organization.

Therefore, the Board recommends that Congress work with the Board to craft legislation that provides limited subpoena authority to the Board, subject to robust controls and protections for subpoenaed parties. A draft bill for Congress's consideration is respectfully attached as Appendix A.

3.2 Mission, Scope, and Responsibilities

EO 14028: "(ii) the Board's proposed mission, scope, and responsibilities"

Recommendation: No changes are recommended to the mission, scope, or overall responsibilities of the Board.

The mission of the Board generally resonated with members, participants, and the broader stakeholder community. The flexibility within the EO gives the DHS Secretary and the CISA Director latitude to assign the Board specific events or, as in this case, critical vulnerabilities. The task process also builds sufficient flexibility to ensure alignment with the mission and responsiveness to the current environment.

3.3 Membership Eligibility Criteria for Private-Sector Representatives

EO 14028: "(iii) membership eligibility criteria for private-sector representatives"

Recommendation: No changes should be made to eligibility criteria.

The Board believes that its members represent the appropriate expertise and seniority as representatives of federal agencies and private-sector organizations. The cybersecurity community was generally impressed with the caliber, seniority, and prominence of both the public and private sector members.

3.4 Governance Structure

EO 14028: "(iv) Board governance structure including interaction with the executive branch and the Executive Office of the President"

Recommendation: No changes to the Board governance structure should be made and the Board's independence should be maintained.

As it did during its inaugural review, the CSRB must continue to be able to operate as an independent body resourced by DHS/CISA. Generally, the CSRB should be able to call upon executive branch agencies or the Executive Office of the President to provide information needed to support a particular review. Notwithstanding, we believe the Board should be an independent body insulated in how it chooses to conduct a review so that its work and judgments are free from actual or perceived interference from any federal agency, to include its own supporting agency. The Board recommends that its leadership engage with the DHS Office of the General Counsel to identify any additional protocols that will ensure these objectives are met in future reviews.

3.5 Thresholds and Criteria for Evaluation of Cyber Incidents

EO 14028: "(v) thresholds and criteria for the types of cyber incidents to be evaluated"

Recommendation: No changes should be made to the thresholds and criteria for the types of cyber incidents to be evaluated.

The Board believes the evaluation criteria outlined in EO 14028 are generally effective. The EO directs the CSRB to "review and assess, with respect to significant cyber incidents (as defined under Presidential Policy Directive 41 of July 26, 2016 [the United States Cyber Incident Coordination] [PPD 41])…at any time as directed by the President acting through the APNSA; or at any time the Secretary of Homeland Security deems necessary." This framing gives the President, the Secretary of Homeland Security, and the CISA Director adequate and appropriate flexibility to task the CSRB as circumstances arise, including events ranging from significant compromises to vulnerabilities and remediations. The Board does not recommend establishing additional bright line thresholds or criteria for when the Board should conduct a review. Instead, the Board recommends maintaining senior executive branch leadership's reasonable discretion to select those incidents where the Board could provide valuable insight, review, and recommendations.

Recommendation: The Board should establish criteria for the management of reviews based on the scope, complexity, and available data for the event.

The Board believes it would be well-served by the establishment of additional formal protocols and procedures to guide the management of a review following its initiation, to include requests for information, review of classified material, and live interview candidates.

3.6 Necessary Sources of Information

EO 14028: "(vi) sources of information that should be made available to the Board, consistent with applicable law and policy"

Recommendation: The Board should establish methods for the collection of information through public data calls.

The establishment of procedures and tools to collect data through public data calls would provide an additional information source. Soliciting input from the public may be valuable in certain instances to the Board's fact-finding or development of recommendations. The Board did not have such a procedure readily available during its inaugural review but recommends developing one together with CISA to support future reviews.

Recommendation: The Board should establish procedures with the Intelligence Community to facilitate the receipt of intelligence related to a review.

The Board was able to productively receive intelligence assessments from the Intelligence Community during the initial Log4j review. This was done on an ad hoc basis and served the needs of the review underway, but the Board believes that regular access to intelligence, appropriate to clearance levels, is important to ensure members have a full understanding of the events and data surrounding a review. The Board should work with the Intelligence Community to establish procedures for receiving intelligence briefings at the initiation of a review and processes for requesting additional intelligence during the review period.

3.7 Approach for Information Protection

EO 14028: "(vii) an approach for protecting the information provided to the Board and securing the cooperation of affected United States individuals and entities for the purpose of the Board's review of incidents"

Recommendation: The Board should establish policies, processes, and (where necessary) memoranda of understanding with federal and non-federal entities regarding Board access to and handling of classified, traffic light protocol (TLP), proprietary, and other sensitive information relevant to their review of significant cyber events.

During the Log4j review, the Board found that its approach to handling sensitive information was sensible, but developed ad-hoc based on existing CISA information handling and protection regimes. The Board believes that the development of a CSRB-specific data acquisition and management plan, which includes policies, standards, and processes for the handling of information, is advisable. The plan should include, but not be limited to, procedures for securely storing and sharing Board data amongst members and staff.

Recommendation: The Board should communicate standards and procedures for information protection.

Following the establishment of data acquisition and management policies, standards, and processes, the Board should establish standards for the distribution of information within the Board and support staff, consistent with any ethics or recusal guidance and procedures for information sharing across federal entities. The communication of these standards and procedures will help the Board build trust with the stakeholder community and increase the likelihood of voluntary participation in information requests in the future. The Board should provide the stakeholder community with the standards and procedures prior to requesting information.

Recommendation: A member of the Board staff should be formally assigned as its data acquisition and management officer.

The Board recommends the development of data acquisition and management policies, standards, and processes. Designating a member of the Board staff to serve as the Officer in charge of data acquisition and management would ensure a continued focus on the issue of information protection and provide for a single point of contact should any questions arise.

3.8 Administrative and Budgetary Considerations

EO 14028: "(viii) administrative and budgetary considerations required for operations of the Board"

Recommendation: Staffing levels should be increased to support the institutionalization of the Board and future reviews.

The Board believes that it was not adequately supported from a staffing perspective during its first review. Members, all of whom are senior executives within the government or private sector, managed to fill staffing gaps on their own time, but that is not a sustainable solution. The CSRB Charter executed by the Secretary of Homeland Security calls for CISA to provide five full-time employees to support the operations of the Board; CISA and the Board should work together to assign those staff promptly.

In addition to permanent federal staff, CISA should support the Board in adopting processes to support efficient onboarding (to include appropriate security clearances) of additional Special Government Employees, subject matter experts, and federal detailees.

Recommendation: Review timelines should be dependent upon the complexity of the event under review.

The 90-day timeline required by the EO for the inaugural review was extremely constrained. The Board assessed it could not conduct a review within that period and that additional time was required to conduct a high-quality process, follow the facts wherever they may lead, and develop thoughtful recommendations and written product. Ultimately, the Board required nearly 136 days to complete its work fully.

The Board requires the ability to set aspirational timelines based on the particular event under review. Based on the initial review, the Board believes a 120-day target for subsequent reviews is an appropriate goal, while maintaining flexibility to take longer if required to conduct a meaningful and careful review. The Board observes that the EO's 90-day delivery requirement applied only to the inaugural review and not to future reviews. In all events, the Board will take the time required to ensure its work is thorough.

Recommendation: The Board should work with congressional and executive branch stakeholders to create a model for sustainable and predictable appropriations.

While the Board believes the best option for ensuring sustainable appropriations is codification of its role within legislation, in lieu of that, DHS/CISA and OMB should work together to mature the annual budget request to secure steady and sustainable appropriations for the Board to enable forward planning. The Board recommends that its leadership engage with appropriate officials at DHS/CISA and OMB, as well as appropriate congressional committees, to formulate a proposed, sustainable appropriations model for the Board's future operations.