UNITED STATES DEPARTMENT OF HOMELAND SECURITY

CYBER SAFETY REVIEW BOARD CHARTER

1. Committee's Official Designation:

Cyber Safety Review Board (CSRB)

2. Authority:

Pursuant to section 5 of Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*, dated May 12, 2021, and section 871(a) of the *Homeland Security Act of 2002*, 6 United States Code (U.S.C.) § 451(a), the Secretary of Homeland Security [hereinafter referred to as the "Secretary"] in consultation with the Attorney General hereby establishes the CSRB for the purposes set forth herein. In recognition of the sensitive nature of the subject matter involved, the Secretary hereby exempts the CSRB from Public Law 92-463, *The Federal Advisory Committee Act* (FACA), 5 U.S.C. App.

3. Objectives and Scope of Activities:

The CSRB shall review and assess, with respect to significant cyber incidents (as defined under Presidential Policy Directive 41 (PPD-41), *United States Cyber Incident Coordination,* of July 26, 2016) affecting Federal Civilian Executive Branch (FCEB) Information Systems or non-Federal systems, threat activity, vulnerabilities, mitigation activities, and agency responses. Members will have access to classified and unclassified information during the review and assessment process, consistent with the need to protect sensitive sources and methods as necessary to effectively undertake particular reviews.

4. Description of Duties:

The duties of the CSRB are solely advisory in nature, as established under EO 14028, *Improving the Nation's Cybersecurity*, dated May 12, 2021, and section 871(a) of the *Homeland Security Act of 2002*, 6 U.S.C. § 451(a).

5. Officials to Whom the Committee Reports:

The CSRB will advise, report to, and make independent, strategic, and actionable recommendations to the Secretary through the Director of the Cybersecurity and Infrastructure Security Agency (CISA).

6. Member Composition:

The CSRB shall be composed of no more than 20 standing members who are appointed by the CISA Director. Membership shall include at least one representative from the Department of Defense, the Department of Justice, Department of Homeland Security (DHS), CISA, the National Security Agency, and the Federal Bureau of Investigation. A representative from the Office of Management and Budget shall

participate in CSRB activities when an incident under review involves FCEB Information Systems. Additionally, the CISA Director shall appoint individuals from private sector entities to include appropriate cybersecurity or software suppliers. The CISA Director will coordinate with the DHS Under Secretary for Strategy, Policy, and Plans in selecting representatives for the CSRB.

Appointments shall be made without regard to political affiliation. Members shall operate in their personal capacity and, as such, will be expected to bring independent expertise to the CSRB rather than reflecting the equities of any current or previous employer or sector.

To aid in the review of specific incidents under review the CISA Director may invite the participation of others on a case-by-case basis depending on the nature of the incident. Such participants may serve as members or be asked to provide information and input to inform the members' development of advice, information, and recommendations of the CSRB.

Members who are not Federal employees will be appointed as expert and consultants pursuant to 5 U.S.C. § 3109 and serve as Special Government Employees (SGE) as defined in 18 U.S.C. § 202(a) and must complete New Entrant U.S. Office of Government Ethics (OGE) Form 450 financial disclosure reports and ethics training annually. Members may be required to sign a non-disclosure agreement (NDA). Members may also be required to obtain a security clearance.

The terms of SGE members shall be two years, renewable up to three times, except that a member may continue to serve until a successor is appointed. SGE appointments are personal to the member and cannot be transferred to another individual or other employees of the member's organization of employment. Members of the CSRB may not receive pay or benefits from the United States Government by reason of their service on the CSRB. In the event the CSRB terminates, all appointments to the board shall terminate.

For the CSRB to fully leverage broad-ranging expertise and perspectives, the membership should be diverse.

Officers:

The CISA Director shall biennially designate a Chair and Deputy Chair from among the members of the CSRB. The Chair shall be a Federal official, and the Deputy Chair shall be a private-sector member. The DHS Under Secretary for Strategy, Policy, and Plans shall serve as the initial DHS member of the CSRB and furthermore serve as the inaugural Chair for the first two-year term. The Deputy Chair will act as Chair in the absence or incapacity of the Chair or in the event of a vacancy in the office of the Chair, until a new Chair is appointed. The Chair or Deputy Chair shall preside at all full meetings of the CSRB.

Reports:

Following completion of a review and assessment of an incident, the CSRB Chair shall deliver the final report to the CISA Director to transmit, unaltered, to the Secretary, to include both findings and recommendations. A majority of CSRB members must agree by vote to submit the report. Any member or members may submit a minority report, which shall be attached to the majority report that is transmitted to the Secretary by the CISA Director.

The CSRB shall protect sensitive law enforcement, operational, business, and other confidential information, consistent with applicable law. The report may include a classified annex to include classified material and other sensitive nonpublic information that is protected from public release. Whenever possible, a version of the report will be made available, with any appropriate redactions, consistent with applicable law and the need to protect sensitive information from disclosure. The CSRB will only include non-public information in the public report with the express, written consent from the entity with control of the information.

The CSRB may also deliver interim reports and recommendations to the Secretary through the CISA Director when the CSRB determines by a vote that doing so may be in the interest of national security.

The Secretary, in consultation with the Attorney General, shall provide to the President, through the Assistant to the President for National Security Affairs (APNSA), any advice, information, and recommendations of the CSRB for improving cybersecurity and incident response practices and policy upon completion of the CSRB's review of an applicable incident.

7. Subcommittees:

At the request of the CISA Director or the Chair, the DFO may establish subcommittees, task forces, or working groups (collectively referred to as "subcommittees") for any purpose consistent with this charter. In the event the subcommittee or CSRB terminates, all appointments to the subcommittee shall terminate. Subcommittees are responsible for executing the CSRB's directed tasks and reporting results to the CSRB.

Subcommittees shall be composed of at least two CSRB members and subject matter experts relevant to the matter before the subcommittee. The DFO, in consultation with the Chair and the CISA Director shall designate a Chair and Deputy Chair for each of the subcommittees from among the CSRB's members. Subcommittees may not work independently of the CSRB and must present their advice or work to the CSRB for full deliberation and discussion. Subcommittees have no authority to make decisions on behalf of the CSRB and may not report directly to any entity other than the CSRB. Subcommittee members may be required to sign an NDA and may need to be appointed as experts and consultants.

8. Ethics Requirements:

Individuals participating in the CSRB or any subcommittee of the CSRB are subject to the Federal conflict of interest statutes, and shall avoid taking any action that would result in an actual or perceived conflict of interest related to any non-governmental entity. CSRB or subcommittee members will refrain from using any information obtained solely by virtue of their participation in the CSRB or any subcommittee of the CSRB for the benefit of external parties, including but not limited to their employer, organizations they are affiliated with in a personal capacity, or themselves personally. Such information includes, but is not limited to, classified, proprietary, procurement-sensitive, and non-public information. Failure to adhere to this requirement may result in consequences that include, but are not limited to, removal from and serve as a potential bar against future participation in the CSRB, for the individual and for the individual's employer. Finally, CSRB members could be subject to criminal penalties should their actions be found to violate any of the Federal conflict of interest statutes.

CSRB or subcommittee members will disclose to the DFO any potential conflict of interest that may affect their own impartiality, or external parties, including but not limited to their employer, organizations with which they are affiliated in a personal capacity, or themselves, in offering recommendations or other information. The DFO will be responsible for addressing conflicts of interest. For this purpose, potential conflicts of interest include an individual who:

- Is actively pursuing a government contract, grant, or other Federal award or funding directly related to the subject matter area in which the participant is offering recommendations as part of the CSRB;

- May have impaired objectivity in providing advice (e.g., participant provides recommendations that include assessments of itself or of a competitor); and

- May obtain an unfair advantage by virtue of their participation in the CSRB (e.g., participant provides technical recommendations that inform procurement efforts and the participant subsequently submits a proposal to fulfill that requirement).

9. Estimated Number and Frequency of Meetings:

The CISA Director shall convene the CSRB following a significant cyber incident triggering the establishment of a Cyber Unified Coordination Group as provided by section V(B)(2) of PPD-41; at any time as directed by the President acting through the APNSA; or at any time the Secretary or CISA Director deems necessary.

10. Voting Procedures:

Only CSRB members may vote. For matters requiring a vote of the CSRB, the CSRB Chair calls for a motion, requests a second for the motion, and then calls for the members to vote for or against the motion after appropriate deliberation. All matters requiring a vote by the CSRB are recorded in the official minutes of the meeting. All issues will be decided, and recommendations or decisions made (to include a vote to submit a report under section 6 of this Charter), by a majority vote of the CSRB members.

11. Agency Responsible for Providing Necessary Support:

The CISA Director shall be responsible for administratively managing, supporting, and funding the CSRB.

12. Estimated Cost, Compensation, and Staff Support:

The estimated annual cost of operating the CSRB is approximately $2,800,000, which includes administrative expenses, contract support, and five Full-Time Equivalent employees to support the CSRB.

13. Designated Federal Officer:

The CISA Director shall appoint full-time permanent employees to serve as the Designated Federal Officer (DFO) and Alternate DFOs (ADFO). The DFO or ADFO shall approve and schedule all CSRB meetings at the request of the Chair, approve meeting agendas, attend all CSRB and subcommittee meetings, adjourn any meeting when the DFO determines adjournment is appropriate, chair meetings in the absence of the Chair and Deputy Chair, and submit reports to the Secretary.

The DFO may review the participation of a member of the CSRB and recommend removal to the CISA Director of such member any time at his/her discretion to include for violation of established responsibilities as outlined in the CSRB Charter or any CSRB bylaws.

14. Recordkeeping:

The records of the CSRB and any established subcommittees shall be handled in accordance with General Records Schedule 6.2, or other applicable and approved agency records disposition schedule. These records shall be available for public inspection and copying in accordance with the *Freedom of Information Act (FOIA),* 5 U.S.C. § 552, subject to any applicable FOIA exemptions or exclusions.

15. Duration and Termination:

The CSRB shall function on a continuing basis until the earlier of (A) two years from the date of renewal indicated below; or (B) termination by the Secretary. This charter is in effect for two years and may be amended at any time at the discretion of the Secretary, or renewed at the end of this two-year period pursuant to section 871 of the Homeland Security Act of 2002, 6 U.S.C. § 451(a), as amended, and section 5 of EO 14028.

Alejandro N. Mayorkas
Secretary of Homeland Security
Date: September 21, 2021