CHARTER

Cybersecurity Forum for Independent and Executive Branch Regulators

I. Purpose and Scope

Cyber threats to U.S. government agencies and domestic industry across all sectors are persistent and evolving. These threats are dynamic and multi-dimensional due to the continuously evolving capabilities of potential adversaries and emerging technologies.

The purpose of this voluntary Cybersecurity Forum for Independent and Executive Branch Regulators (Forum) is to increase the overall effectiveness and consistency of regulatory agency cybersecurity efforts pertaining to U.S. Critical Infrastructure, which is owned and operated by public and private entities that are overseen by a number of federal regulatory authorities.

The Forum will identify and explore opportunities to promote unity of effort across participant agencies, as well as to leverage and deconflict cross-sector regulatory authorities' approaches to strengthen our nation's cybersecurity posture. By coordinating strategic objectives and priorities, the Forum will focus on incentivizing and requiring public-private organizations to implement more robust cybersecurity risk management measures/best practices and accountability methods.

II. Objectives:

a. Identifying gaps in existing policy, regulatory authority, and regulations associated with critical infrastructure, and assessing potential clarifications or revisions to include consideration of interdependencies and Information Technology/Operational Technology interdependencies.

b. Pursuant to existing authorities, exploring possible approaches to developing or revising regulations that may ultimately be considered by individual agencies to reduce cyber risk to critical infrastructure, while avoiding undue burden to regulated entities.

c. Identifying common objectives that Federal regulators could consider through current or new cybersecurity regulatory frameworks -- leveraging resources such as the NIST Cybersecurity Framework, the CISA Cybersecurity Performance Goals and recognized cybersecurity standards, guidance, and outcomes -- to oversee the management of cybersecurity risks across private-sector organizations.

d. To the extent possible, harmonizing regulation and regulatory activities among agencies to achieve greater cross-sector risk management, promote greater cybersecurity assurance, incorporate privacy and data protection, and enhance cybersecurity oversight. For example:

    i. Coordinating regulatory and administrative requirements, such as audits, reporting, vulnerability assessments, breach and incident disclosures, CISA programs, and/or subsidies to reduce the costs and burdens associated with implementing cybersecurity

requirements;

ii. Identifying approaches that promote stronger public-private partnerships and assist in assessing the costs and benefits of cybersecurity investments; and

iii. Creating ideas for incentives designed to promote cross-sector cybersecurity, such as participation in voluntary cybersecurity programs.

e. Expanding opportunities for Independent- and Executive-Branch regulators to collaborate with Sector Risk Management Agencies (SRMAs) pursuant to National Security Memorandum 22.

f. Understanding regulators' ability to implement and oversee cybersecurity regulations and what, if any, technical assistance they may need from other Departments and Agencies.

g. And any other objectives to which the Forum members agree.

IV. Membership

Federal regulators are eligible to be members of the Forum. Other entities may participate as advisors. The following independent regulators and Executive Branch entities are represented on the Forum at the Principal level:

- Federal Communications Commission (Chair)
- Commodity Futures Trading Commission
- Consumer Product Safety Commission
- Federal Energy Regulatory Commission
- Department of Health and Human Services / Food and Drug Administration
- Department of Health and Human Services / Office for Civil Rights
- Department of Homeland Security / Cybersecurity and Infrastructure Security Agency
- Department of Homeland Security / Transportation Security Administration
- Department of Homeland Security / U.S. Coast Guard
- Department of Transportation / Federal Aviation Administration
- Department of Treasury / Office of the Comptroller of the Currency
- Environmental Protection Agency
- Federal Deposit Insurance Corporation
- Federal Housing Finance Agency
- Federal Maritime Commission
- Federal Reserve Board
- Federal Trade Commission
- National Association of Insurance Commissioners
- National Credit Union Administration
- Nuclear Regulatory Commission
- Securities and Exchange Commission
- Surface Transportation Board
- Other Independent and Executive Branch regulators, as appropriate

The following organizations serve as Advisors to the Forum:

- Department of Treasury
- Office of Management and Budget
- Department of Commerce / National Institute of Standards and Technology
- Department of Commerce / National Telecommunications and Information Administration
- Department of Justice
- National Security Council
- Office of the National Cyber Director
- Department of Homeland Security

V. Decision-making Process

The Forum uses a collaborative, problem-solving approach in its work. Working Groups will strive for understanding among participating members. Members will work by consensus to perform the administrative functions (agendas, meeting schedules, etc.) as well as to achieve operational goals. Consensus is defined as decisions that all participants can "live with." To the extent there are dissenting views, they should be noted in meeting summaries and/or documents produced.

VI. Working Groups

As may be required, the Forum Chair, in close consultation with the Forum members, will establish standing working groups, and then focused working groups, as needed, and designate the working group chairs.

VII. Staff-level Support

Each of the member agencies will designate a senior staff member who will coordinate the activities and complete the work of the Forum and any associated working groups. Subject matter experts from member agencies and advisors may participate in working groups, as needed; however, these individuals would not participate in Forum decision-making. Staff from the Chair's Agency will provide the administrative functions of the Forum, including overseeing day-to-day operations of the Forum. The staff will ensure that meeting agendas and supporting materials are distributed at least one week prior to meetings and coordinate any conference calls. The staff will also prepare and provide summaries of key discussion points and any action items arising from discussions to Forum members.

VIII. Security

In recognition of the sensitive nature of information surrounding cybersecurity, particularly involving system and component vulnerabilities, the Forum will consciously avoid discussions that involve National Security Information (as defined in Executive Order 13526) and Safeguards Information (as defined in the Atomic Energy Act of 1954, as amended), unless appropriate clearances and protective measures are in place, and will take all necessary

precautions to protect information that is deemed sensitive but unclassified, including Controlled Unclassified Information (as defined in Executive Order 13556).

IX. Reporting

The Forum may issue reports, as appropriate. Working groups will provide a report to the full Forum at the conclusion of their work.

X. Freedom of Information

FOIA requests will be handled by the existing processes and procedures of the Forum members.

XI. Schedule and Duration

It is expected that the Principals will meet as needed but not less than once per year. Rotation of the Chair will occur when the agency chairing the Forum announces they would like to relinquish the lead, or when Forum members suggest rotation. In either of such cases, agencies will announce their interest in assuming lead; if a consensus cannot be reached among those interested, discussion among all Forum members will facilitate consensus. The Forum Chair will coordinate with Forum members and advisors to craft and execute the succession process to include transfer of relevant documents and notes.

XII. Private Sector Interface

The Forum can interact with and receive private sector, academic, and nongovernmental advice as needed to carry out its work, consistent with the Federal Advisory Committee Act.

XIII. External Affairs

Should they arise, the public affairs and legislative affairs staff of the Forum Chair's agency will coordinate external affairs matters relating to the Forum with their counterparts in the Forum member agencies. Any media inquiries made to working group members relating to the Forum will be referred to the Forum Chair's public affairs staff, or to such staff of the relevant member agency, for coordination among the Forum members.

XIV. Other Provisions

Nothing in this Charter is intended to conflict with law, regulation, Presidential order or directives of the member agencies. The charter should be interpreted and implemented in a manner that respects, complies with, and does not abrogate the statutory and regulatory responsibilities of the member agencies. Amendments to this Charter may be suggested by any Forum member and implemented upon consensus agreement of Forum Principals.

Cybersecurity Forum for Independent and Executive Branch Regulators
Charter Appendix A
Reference Documents

- Cyber Incident Reporting for Critical Infrastructure Act of 2022, March 12, 2022, https://www.govtrack.us/congress/bills/117/hr2471/text
- Executive Order 13636 – Improving Critical Infrastructure Cybersecurity, February 12, 2013. https://www.federalregister.gov/articles/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity
- Executive Order 13873 - Securing the Information and Communications Technology and Services Supply Chain. https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain
- Executive Order 14028 – Improving the Nation's Cybersecurity, May 12, 2021. https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity
- NIST Framework for Improving Critical Infrastructure Cybersecurity, V 2.0, February 26, 2024. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
- National Security Memorandum 5 on "Improving Cybersecurity for Critical Infrastructure Control Systems," July 28, 2021.
- S. 3600 Strengthening American Cybersecurity Act, March 1, 2022, https://www.congress.gov/bill/117th-congress/senate-bill/3600
- National Security Memorandum 22, "National Security Memorandum on Critical Infrastructure Security and Resilience," April 30, 2024, https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/