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 enhanced capabilities of potential adversaries and emerging technologies.

The purpose of the voluntary Cybersecurity Forum for Independent and Executive Branch Regulators (The Forum) is to increase the overall effectiveness and consistency of regulatory authorities' cybersecurity efforts pertaining to U.S. Critical Infrastructure, much of which is operated by industry and overseen by a number of federal regulatory authorities. The Forum will enhance communication among regulatory agencies and regulated entities through the sharing of best practices and exploring ways to align, leverage, and deconflict approaches to enhance cybersecurity protections, and will establish processes to encourage coordination and consistency where multiple Agencies have regulatory authority over a common industry.

II. Objectives:

The Forum will identify and explore opportunities to align, leverage, and deconflict cross-sector regulatory authorities' approaches and promote cybersecurity protection. The goals of the Forum are the following:

a. Building a shared understanding among participant agencies of current regulatory and voluntary approaches to cybersecurity to inform the work of Forum members in exercising their domestic jurisdictional authorities and their international engagements and coordination;
b. Exploring the challenges of implementing the National Institute of Standards and Technology (NIST) Framework (Framework) and other subject matter expertise;
c. Sharing regulatory best practices;
d. Exploring the efficiency and effectiveness of existing requirements, for example identifying duplicative regulations and ways to decrease undue burdens;
e. Exploring ways to coordinate regulatory activities, risk management and consequence-based approaches to cybersecurity oversight;
f. Exploring ways to streamline, consolidate, and/or improve consistency among multiple-agency (i.e., industry cross-sector) regulatory and administrative requirements (e.g., audits);
g. Identifying appropriate opportunities to align, leverage, and deconflict approaches that promote proactive, market-driven, private-sector leadership in cybersecurity program implementation, including developing meaningful methods of assessing the costs and benefits of cybersecurity investments;
h. Exploring incentives designed to promote participation in voluntary cybersecurity programs, including, e.g., 2013 Executive Order Section 8 (d) Voluntary Critical Infrastructure Cybersecurity Program.
i. Incorporating privacy as a fundamental element of cybersecurity considerations, practices and activities.

j. Identifying and addressing shortfalls regarding cybersecurity threat and vulnerability information and situational awareness, particularly pertaining to interdependencies between different companies, services, or industry sectors.

IV. Membership
The following independent regulators and Executive Branch entities are represented on the Forum at the Principal level:

- Nuclear Regulatory Commission (chair)
- Federal Communications Commission
- Federal Energy Regulatory Commission
- Securities and Exchange Commission
- Federal Trade Commission
- Federal Reserve Board
- Federal Financial Institutions Examination Council
- Financial and Banking Information Infrastructure Committee
- National Association of Insurance Commissioners
- Other Departments may participate as appropriate

The following organization serves as an Advisor to the Forum:

- NIST

V. Decision Making Process
The Forum intends to use a collaborative, problem-solving approach in its work. The workgroup will strive for understanding among participating members. For administrative functions (agendas, meeting schedules, etc.) members will work by consensus. Consensus is defined as decisions that all participants can "live with."

VI. Working Groups
As may be required, the Forum Chair, in close consultation with the Forum members, will establish working groups 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. 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. Subject matter experts from member agencies 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.

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.

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 semi-annually and the staff will direct the day-to-day operations of the Forum, including undertaking any studies. The option of a rotating chair after the initial two-year term may be considered.

XII. Private Sector Interface
The Forum can interact with and receive private sector, academic and nongovernmental advice as needed to accomplish its work, consistent with the Federal Advisory Committee Act.

XIII. External Affairs
Should they arise, the public affairs and legislative affairs staff of the 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.

Reference Documents

- Executive Order 13636 – Improving Critical Infrastructure Cybersecurity, February 12, 2013. https://www.federalregister.gov/articles/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity

- NIST Framework for Improving Critical Infrastructure Cybersecurity, February 2014 http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf