Government Relations Update

NPAG Meeting
October 11, 2022

ANSI WORLD STANDARDS WEEK   FALL 2022

Recent Activities of Note

- Congressional Actions
  - CHIPS and Science and Inflation Reduction Acts passed

- Executive Orders
  - Advancing biotechnology
  - Inbound investment screening

- Updated Administration Approach to Emerging Technology Exports
  - BIS Rule on Standards Participation
  - Scrapping foundational vs. emerging technology definitions

- Enhancing the Security of the Software Supply Chain through Secure Software Development Practices (OMB memo)

CHIPS and Science

- One of six Administration Priorities: Ensure long-term leadership in the sector
  - The CHIPS program will establish a dynamic, collaborative network for semiconductor research and innovation to enable long-term U.S. leadership in the industries of the future.
  - The program will support a diversity of technologies and applications along many stages of product and process development.
- Commerce released its strategy
  - The strategy outlines the initiatives, strategic goals, and guardrails guiding the *CHIPS for America* program.
  - The U.S. Department of Commerce released a summary of responses to a Request for Information (RFI) on incentives, infrastructure, research and development, and workforce needs to support a strong domestic semiconductor industry

Advancing Biotechnology

- On September 12, 2022, President Biden issued [the Executive Order on Advancing Biotechnology and Biomanufacturing Innovation for a Sustainable, Safe, and Secure American Bioeconomy](#).
    - The EO launches a National Biotechnology and Biomanufacturing Initiative to focus federal investments that transform biotechnology discoveries into solutions for critical problems.

- The EO directs NIST, in partnership with federal and other stakeholders, to:
    - Create and make publicly available a lexicon to assist in the development of measurements and measurement methods of the bioeconomy.
    - Take steps to improve the nation's cybersecurity for biological data and bio-related software, consistent with President Biden's Executive Order 14028.

Inbound Investment Screening

- On September 15, 2022, the Biden Administration issued a new [executive order](#) ("EO") and accompanying [fact sheet](#), designed to sharpen the current U.S. foreign investment screening process as administered by the Committee on Foreign Investment in the United States ("CFIUS" or the "Committee").
  - This EO is the first to specifically identify certain additional national security factors for CFIUS to consider when evaluating transactions involving foreign investors.

- While the EO does not expand the jurisdiction of CFIUS or establish new requirements, it formally directs CFIUS to focus on transactions that could give foreign parties access to U.S. technologies, data, or critical supply chains that the Biden Administration has identified as important for maintaining U.S. economic and technological edge.

Emerging Technology Exports

- In 2018, the U.S. enacted a law requiring the Commerce Department to identify so-called emerging and foundational technologies to be restricted from export to hostile nations

- Earlier this year, Commerce's Bureau of Industry and Security, which oversees export controls, formally [announced it would abandon classifying items as "emerging" or "foundational"](#)
  - Instead, recent BIS rules have targeted specific technologies, applying a 'Section 1758 technology' characterization allows BIS to more efficiently identify and control technologies that pose a national security threat

- In May 2019, BIS issued a temporary general license related to 5G technologies and participation in specific standards activities

- In September, BIS issued a new IFR addressing concerns raised by stakeholders, identifying standards participation and leadership as a national security interest

Software Supply Chain Security

- The Office of Management and Budget (OMB) released Memorandum M-22-18, implementing software supply chain security requirements that will have a significant impact on software companies and vendors in accordance with Executive Order 14028, Improving the Nation's Cybersecurity.

- The Memorandum requires all federal agencies and their software suppliers to comply with the NIST Secure Software Development Framework (SSDF), NIST SP 800-218, and the NIST Software Supply Chain Security Guidance whenever third-party software is used on government information systems or otherwise affects government information.

- The term "software" includes firmware, operating systems, applications, and application services (*e.g.*, cloud-based software), as well as products containing software. It is critical to note that these requirements will apply whenever there is a major version update or new software that the government will be using.