U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Director
Washington, DC 20528

April 15, 2024

Mr. Steven Lipner
Chairman
National Institute of Standards and Technology
Information Security and Privacy Advisory Board
100 Bureau Drive
Gaithersburg, MD 20899

Dear Mr. Lipner,

Thank you for your January 10, 2024 letter to Secretary Mayorkas regarding the European Union (EU) Cyber Resilience Act (CRA), which is now awaiting formal adoption by the European Council. The Secretary asked that I respond on his behalf.

The Cybersecurity and Infrastructure Security Agency (CISA) appreciates your concerns while also noting the importance of responsible and timely vulnerability disclosure. We continue to actively engage with colleagues at the European Union Agency for Cybersecurity (ENISA) to discuss the CRA and its implementation. ENISA will be responsible for developing and managing: 1) a public-facing European Vulnerability Database, and 2) a single reporting platform that will be used to report on and receive information about actively exploited vulnerabilities in products with digital elements as well as severe incidents having an impact on the security of those products. Appreciating that the specific vulnerability disclosure requirements in the CRA still need to be developed, our conversations with ENISA include discussions of processes for vulnerability disclosure and management, and the importance of starting with well-established standards and best practices. We will also continue to work with EU Member States and the European Commission to encourage clear scoping of the vulnerability reporting and vulnerability infrastructure requirements under the CRA, as well as the EU Network and Information Security (NIS2) Directive.

As we undertake this collaborative effort, we will continue to seek a balance between the availability of cybersecurity information to drive appropriate mitigation and investment with the need to manage burdens on those organizations and individuals who must design secure products and defend our critical infrastructure. In a geopolitical and technological landscape marked by the proliferation of new threats and malicious actors, it is imperative that we continue to cooperate and join forces to promote our shared values and objectives in cyberspace.

As the European Council approves the final text of the CRA, likely by September 2024, we will continue to work with ENISA and our interagency colleagues to collaborate on the CRA implementation guidance, and, in particular, on vulnerability disclosure and management principles to ensure vulnerabilities are prioritized, disclosed in a coordinated manner, and handled with security and confidentiality in mind.

I appreciate your interest in and concerns regarding the CRA and its impact on our vulnerability disclosure requirements. Should you need additional assistance, please do not hesitate to contact me.

Sincerely,

Jen Easterly
Director