INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987
[Amended by the Federal Information Security Management Act of 2002]

January 10, 2024

Dr. Laurie E. Locascio
Under Secretary of Commerce for Standards
and Technology and Director, National Institute
of Standards and Technology

Dear Dr. Locascio,

I am writing as Chairman of the National Institute of Standards and Technology (NIST) Information Security and Privacy Advisory Board (ISPAB). By statute, the ISPAB is charged with advising NIST, the Secretary of the Department of Homeland Security (DHS), and the Director of the Office of Management and Budget (OMB) on information security and privacy issues pertaining to Federal Government information systems as well as the development of security and privacy standards.

On October 26, 2023, Christiane Kierketerp de Viron, the Head of the European Commission's Unit for Cybersecurity and Digital Privacy Policy, briefed the ISPAB on the proposed European Union (EU) Cyber Resilience Act (CRA). The ISPAB supports efforts to promote more secure hardware and software products and commends the European Parliament and European Commission for adopting common standards across the European market intended to meet this objective. The ISPAB is concerned, however, that the CRA's requirements for early vulnerability disclosure to The European Union Agency for Cybersecurity (ENISA) and EU member states will have the unintended consequence of increasing cybersecurity risk.

We understand that a provisional agreement has been reached between the European Commission, Parliament, and the European Council on November 30, 2023, but that the new draft has not been released. The provisional agreement apparently requires reporting vulnerability disclosures to national Computer Security Incident Response Teams (CSIRTs) rather than to ENISA. Regardless of the agency (ENISA or CSIRT), the CRA's proposed vulnerability disclosure framework is problematic. The potential risks created by the proposal merit further consideration by NIST, DHS, and OMB as the US government engages with the EU on the draft CRA.

Board Secretariat: National Institute of Standards and Technology
100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899-8930
Telephone: 301/975-2938 *** Fax: 301/975-4007

We are concerned about the proposal for four primary reasons.

- CRA fails to consider that even non-detailed, non-technical information about an exploited vulnerability can be leveraged by threat actors and increases risk. In several recent cybersecurity incidents flagging software as vulnerable provided useful information to attackers. This was the case with the SMBv1 protocol that the WannaCry worm exploited.
- CRA fails to consider the significant risk that once shared with a government regulator vulnerability information may be widely disseminated before remediation has been completed by the appropriate entity. This creates an unacceptable level of risk of large-scale vulnerability exploitation. Security standards and industry best practices universally caution that the wider the circle of those who know about an unpatched vulnerability, the greater the risk. ISO standards 29147 and 30111, for example, stipulate that knowledge of vulnerabilities be restricted on a need-to-know basis and limited to only those responsible for remediation.
- CRA fails to consider the potential burden of the reporting requirement on the very resources needed to address the ongoing security risk and remediation efforts. Excessive reporting obligations that do not have clear and demonstrable benefits may undermine the CRA's objective of enhancing security. In addition, an overinclusive or poorly defined reporting standard risks overwhelming ENISA and the EU member states with a flood of low-priority or non-actionable information.
- Finally, ISPAB is concerned that if this requirement is codified in the CRA it will serve as precedent for other countries who may then implement similar requirements, further exacerbating the concerns raised by the vulnerability disclosure provision at issue.

The ISPAB urges NIST, DHS, and OMB to further examine these risks and encourage the EU to reconsider the scope and application of the CRAs vulnerability disclosure requirements. We are available to provide additional information or assistance.

Thank you very much.

Sincerely,

Steven B. Lipner
Chair
Information Security and Privacy Advisory Board

CC: The Honorable Alejandro Mayorkas, Secretary United States Department of Homeland Security, (DHS) and
Shalanda D. Young, Director, Office of Management and Budget (OMB)