INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

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

October 9, 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.

Beginning in early 2024, there has been a great deal of discussion and concern in the Information Technology and cybersecurity communities about NIST's updating and sustainment of the National Vulnerability Database (NVD). The NVD is the authoritative data source for product vulnerabilities, the products they effect, their severity, and their remediation. It is used by IT end user organizations, product and online service developers, and cybersecurity organizations worldwide.

The Board has been following developments related to the NVD since its March 2024 meeting, held a special meeting in May 2024 to receive an update on NIST's progress in responding to delays and resource limitations in keeping the NVD up to date, and received briefings on NVD at its July 2024 meeting from both NIST and CISA. The Board understands that the addition of government and contractor staff at NIST and the complementary efforts by CISA are closing the near-term gap in keeping the NVD up to date.

However, the Board is concerned that the influx of product vulnerabilities is only likely to grow as a result of trends including the deployment of artificial intelligence/machine learning (AI/ML) to search out new vulnerabilities and the growing efforts of additional parties such as the People's Republic of China to find, catalogue, and exploit vulnerabilities. Further, the Board is concerned that US national security interests are challenged when the United States does not

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

have a current and accurate record of vulnerabilities impacting United States critical infrastructure and consumers alike.

It is vital that the government have an approach to supporting the NVD that is both timely and scalable. Increasing the number of CVE Naming Authorities (CNAs) that are allowed to create NVD entries – a process that is well underway – is an important part of the solution to the scalability problem but the government must still exercise control to assure the completeness and accuracy of CNA-contributed information. Automation and perhaps the use of AI/ML to make this assurance scalable may be an effective option.

The Board recommends that:

- NIST and CISA continue to provide sufficient resources to keep the NVD current and accurate and avoid the recurrence of a major backlog in updating the NVD.
- NIST and CISA establish effective selection and quality assurance processes to ensure that CNA-contributed NVD entries are timely and trustworthy. NIST and CISA should reach out to the CNA community to develop approaches to training and assurance that scalable, cost-effective and enable timely updating of the NVD.
- NIST initiate research and testing programs to develop options for automating the NVD creation or quality assurance processes with the aim of enhancing the timeliness, accuracy, and scalability of the NVD maintenance process.
- NIST and CISA initiate research and engagement with the CNA community to anticipate future changes and impacts in the NVD space, so that future iterations of the NVD do not reach crisis proportions but are managed with an eye towards product, service, and technology lifecycles.

The Board will continue to track the status of efforts on NVD and is happy to discuss our observations and recommendations at a future meeting.

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)