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 5, 2022

Dr. James Olthoff
Performing the Non-Exclusive Functions and Duties of the
Undersecretary of Commerce for Standards and Technology &
Director, National Institute of Standards and Technology

Dear Dr. Olthoff,

I am writing to you as the Chair of the Information Security and Privacy Advisory Board (ISPAB). The ISPAB was originally created by the Computer Security Act of 1987 (P.L. 100-235) as the Computer System Security and Privacy Advisory Board, and amended by Public Law 107-347, The E-Government Act of 2002, Title III, and The Federal Information Security Modernization Act (FISMA) of 2014. The statutory objectives of the Board include identifying emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy.

At meetings in June, September, and December 2021, the ISPAB received several briefings on Executive Order 14028 and on NIST, CISA, and OMB plans for implementing the Executive Order. The ISPAB was impressed with the scope of the Executive Order and by the approach that it directs agencies to take to improve the cybersecurity of government systems. Full implementation of the Executive Order will undoubtedly make government systems a much harder target for the Nation's adversaries. Implementation of the Executive Order will also make government systems a good example for the private sector to emulate.

On reviewing the Executive Order and the plans for its implementation, the ISPAB was concerned about the magnitude of the effort that the Executive Order will require from government agencies and private sector suppliers and the time it will take to apply that effort. To take only a few examples, agencies will not be able to make their transitions to "Zero-trust" networks, effective sharing of threat information, and a standardized approach to incident response instantly. Many private sector software vendors will have to make major changes to integrate secure development practices into their development lifecycles. The Executive Order is right to insist that these changes be made, but the Government will need improved cybersecurity well before every agency or vendor can meet every requirement. The Executive Order does not exist in a vacuum. There are cybersecurity requirements beyond those of the Executive Order and it should be considered as one part of a more comprehensive, multi-year, government-wide cybersecurity effort.

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

Given these considerations, the ISPAB would like to understand how NIST, CISA and OMB are helping agencies and vendors prioritize their steps to implement the requirements in the Executive Order and related government cybersecurity initiatives. Are the agencies being provided with guidance on resource allocation and which of the many mandatory efforts will have the greatest short-term and long-term impact? For example, agencies should not wait to deploy two-factor authentication until they have completed a transition to Zero-trust architecture. Similarly, it may be prudent for vendors to initially focus on using Software Bills of Materials as part of their own secure development processes rather than waiting to create SBOMs until end-user organizations are prepared to consume them. While SBOM is an important element of an effective software supply chain security program it alone is insufficient and NIST should encourage organizations to adopt broader and more comprehensive frameworks as well. Requirements for compliance documentation should be scoped to rely on artifacts generated during system development and administration (e.g., commit logs, code changes) rather than requiring substantially new documentation processes.

Implementation guidance of the sort described above should consider the results of the recent FedRAMP study (https://www.fedramp.gov/assets/resources/documents/Threat-Based_Risk_Profiling_Methodology.pdf) whose results identify those security controls and capabilities that are most effective in protecting, detecting, and responding to prevalent threats, Such guidance should also undergo continuous improvement as experience and data dictate. The findings of the Cyber Safety Review Board created by the Executive Order can be a great source of lessons learned to be reflected in updated guidance provided to agencies.

Finally, the Executive Order, like many other cybersecurity initiatives, provides that the Heads of the Federal Civilian Executive Branch (FCEB) Agencies are responsible for the security posture of the Agency and must make cybersecurity a priority. The ISPAB would like to understand how the Heads of Agencies are being held accountable for these responsibilities.

We know that NIST, CISA and OMB share our concern and have taken steps to assist agencies in prioritizing their cybersecurity efforts. The ISPAB would appreciate hearing from NIST, CISA, and OMB about these efforts.

Thank you very much.

Sincerely,

Steven B. Lipner
Chair
Information Security and Privacy Advisory Board

CC: Secretary Mayorkas, United States Department of Homeland Security,
Ms. Shalanda D. Young, Acting Director, Office of Management and Budget