Mark R. Warner
US Senator from the Commonwealth of Virginia

The *Secure Artificial Intelligence Act of 2024*

Senator Mark Warner & Senator Thom Tillis

Background

Vulnerability and incident tracking play a crucial role in mitigating cybersecurity risks for organizations. Identification and management of vulnerabilities enables organizations to proactively address security weaknesses and prioritize fixes. Systematic documentation of security incidents and near-misses enables organizations to identify trends, troubleshoot recurring issues, and prevent future incidents. Incident reporting has also helped create and deepen safety cultures in key industries, such as aviation. In the information security context, voluntarily sharing of vulnerabilities and incidents allows organizations to contribute to improving the security of the cyber ecosystem. Further, this voluntary sharing enables those with cybersecurity expertise to provide tailored guidance for protecting vulnerable systems.

The National Institute of Standards and Technology (NIST) and the Cybersecurity and Infrastructure Security Agency (CISA) already play a crucial role in tracking of cybersecurity vulnerabilities through their National Vulnerability Database (NVD) and the Common Vulnerabilities and Exposures Program (CVE), respectively. These programs enable public sharing of security vulnerabilities and are widely used. The National Security Agency (NSA), through the Cybersecurity Collaboration Center, provides intel-driven cybersecurity guidance for emerging and chronic cybersecurity challenges through open, collaborative partnerships.

While AI systems resemble traditional enterprise software in many respects, the unique nature of their development, maintenance, and deployment can raise novel safety and security concerns. As NIST notes in their *AI Risk Management Framework,* AI risks differ from traditional software risks in key ways – including increased opacity and barriers to reproducibility, complex and non-deterministic system dependencies, more nascent testing and evaluation frameworks and controls, and a "higher degree of difficulty in predicting failure modes" for so-called "emergent properties" of AI systems.

When it comes to security vulnerabilities and incidents involving artificial intelligence (AI), existing federal organizations are poised to leverage their existing cyber expertise and capabilities to provide critically needed support that can protect organizations and the public from adversarial harm. The *Secure Artificial Intelligence Act* ensures that existing procedures and policies incorporate AI systems wherever possible – and develop alternative models for reporting and tracking in instances where the attributes of an AI system, or its use, render existing practices inapt or inapplicable.

Summary

Managing AI risk requires collaboration across industry, academia, civil society, and government. As development and use of AI grow, so too does the potential for security and safety incidents that harm organizations and the public. To improve the tracking and processing of security and safety incidents and risk associated with AI, this bill:

- Requires NIST to update the NVD and requires CISA to update the CVE program or develop a new process to track voluntary reports of AI security vulnerabilities.
- Establishes a public database to track voluntary reports of AI security and safety incidents.

- Creates a multi-stakeholder process that encourages the development and adoption of best practices that address supply chain risks associated with training and maintaining AI models.
- Establishes an Artificial Intelligence Security Center at the NSA to provide an AI research test-bed to the private sector and academic researchers, develop guidance to prevent or mitigate counter-AI techniques, and promote secure AI adoption.