Mark R. Warner
US Senator from the Commonwealth of Virginia

Federal Contractor Cybersecurity Vulnerability Reduction Act *of 2024*

Background

Vulnerability disclosure policies (VDPs) provide a way for organizations to receive unsolicited reports of vulnerabilities so that they can be patched. Publicly defining how they will accept, assess, and manage vulnerability disclosure reports through the establishment of these policies enables and encourages good faith researchers to responsibly report vulnerabilities before they are exploited by malign actors. Crowdsourcing reports on suspected security vulnerabilities in information systems is an easy and impactful way for services to become aware of security issues before they become a problem. Through a CISA Binding Operational Directive, all civilian federal **agencies** are required to have VDPs that do just this. However, there is currently no federal requirement for federal **contractors** – civilian or defense – to have VDPs for the information systems used in the fulfillment of their contracts.

Without a VDP, security researchers with an interest in reporting vulnerabilities to protect the public may **NOT**:

- Know how to report discovered vulnerabilities and may choose not to, if doing so is too difficult.
- Have confidence that the vulnerability will be fixed, which could result in them engaging in uncoordinated public disclosure to motivate a fix and leaving the organization vulnerable without time to patch.
- Report the vulnerability in fear of legal action being taken against them.

Summary

The importance of VDPs for federal contractors is most notable when considering the devastating Office of Personnel Management (OPM) data breach of 2014. The attackers were able to breach two contractors, USIS and KeyPoint, who conducted background checks on government employees and had access to OPM servers. By requiring contractors to establish VDPs, good-faith security researchers can report identified vulnerabilities directly to the contractor, without requiring any additional reporting to a federal agency. The national security impact of requiring these policies for all federal contractors could be tremendous. Specifically, this bill requires:

1. OMB to lead updates to the Federal Acquisition Regulation (FAR) to ensure federal contractors implement a vulnerability disclosure policy consistent with what is already required by federal agencies.
2. The Secretary of Defense to lead updates to the Defense Federal Acquisition Regulation Supplement (DFARS) contract requirements to ensure defense contractors implement the same.