Legislation Recommendation 4.1.1 - Critical Technology Security Centers

Introduction to Proposal. This proposal should direct and appropriate funds for the Department of Homeland Security to competitively select, designate, and fund up to three Critical Technology Security Centers in order to centralize efforts directed toward evaluating and testing the security of devices and technologies that underpin our networks and critical infrastructure.

Legend. This proposal would amend existing laws, and therefore changes are highlighted**.**

SEC. XXX. DEPARTMENT OF HOMELAND SECURITY CRITICAL TECHNOLOGY SECURITY CENTERS.

(a) In General.—Title III of the Homeland Security Act of 2002 (6 U.S.C. 181 et seq.) is amended by adding at the end the following:

"SEC. 322. CRITICAL TECHNOLOGY SECURITY CENTERS.

"(a) Definitions.—In this section—

"(1) the term 'Agency' means the Cybersecurity and Infrastructure Security Agency;

"(2) the term 'appropriate committees of Congress' means the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate;

"(3) the term 'Director' means the Director of the Agency;

"(4) the term 'open source software' means software for which the human-readable source code is freely available for use, study, re-use, modification, enhancement, and re-distribution by the users of such software; and

"(5) the term 'Under Secretary' means the Under Secretary for Science and Technology.

"(b) Critical Technology Security Centers Established.—The Under Secretary shall designate cybersecurity-focused Critical Technology Security Centers to evaluate and test the security of devices and technologies that underpin national critical functions.

"(c) Initial Centers.—Of the Critical Technology Security Centers described in subsection (b), the Under Secretary shall designate at least 4, to include—

"(1) the Center for Network Technology Security, to study the security of information and communications technology that underpins national critical functions related to communications;

"(2) the Center for Connected Industrial Control System Security, to study the security of connected programmable data logic controllers, supervisory control and data acquisition servers, and other networked industrial equipment;

"(3) the Center for Open Source Software Security, to study vulnerabilities in open source software used to support national critical functions and coordinate vulnerability remediation efforts; and

"(4) the Center for Federal Critical Software Security, to study the security of software used by the Federal Government that performs functions critical to trust (such as affording or requiring elevated system privileges or direct access to networking and computing resources).

"(d) Additional Centers.—The Under Secretary may, in coordination with the Director, designate additional Critical Technology Security Centers to address technologies vital to national critical functions.

"(e) Designation of Centers.—The Under Secretary shall—

"(1) designate Critical Technology Security Centers based on applications submitted by institutions of higher education (as defined in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001)) or Federally-funded research and development centers, including national laboratories, or consortia thereof; and

"(2) distribute funds through grants, cooperative agreements, and contracts.

"(f) Responsibilities of Centers.—In studying the security of technologies within the area of responsibility of the Critical Technology Security Center, a Critical Technology Security Center shall—

"(1) conduct rigorous security testing to identify vulnerabilities in such technologies;

"(2) report new vulnerabilities found and the tools, techniques, and practices used to uncover them to the developers of the technologies in question and to the Agency;

"(3) develop new capabilities for vulnerability discovery, management, and mitigation within such technologies;

"(4) assess the security of software essential to national critical functions;

"(5) support existing communities of interest, including by granting funds, in remediating vulnerabilities discovered within such technologies; and

"(6) utilize findings to inform and support the work of the Agency;

"(g) Selection of Critical Technologies.—Before distributing funds, the Under Secretary shall consult with the Director, who shall provide the Under Secretary with a list of technologies within the area of responsibility of each Critical Technology Security Center that support national critical functions.

"(h) Biannual Reports.—Not later than 1 year after the date of enactment of this section, and every 2 years thereafter, the Under Secretary shall submit to the appropriate committees of Congress a report containing—

"(1) a summary of the work performed by each Critical Technology Security Center, including an explanation of how grant funding was allocated and a list of vulnerabilities found, along with the corresponding software weakness and an assessment of the criticality

and severity of each vulnerability;

"(2) a list of critical technologies studied by each Critical Technology Security Center, including an explanation by the Under Secretary for any deviations from the list of technologies provided by the Agency before the distribution of funding to the Critical Technology Security Center; and

"(3) a list of tools techniques, and procedures used by each Critical Technology Security Center.

"(i) Authorization of Appropriations.—To carry out this section, there are authorized to be appropriated—

"(1) $40,000,000 for fiscal year 2022;

"(2) $42,000,000 for fiscal year 2023;

"(3) $44,000,000 for fiscal year 2024;

"(4) $46,000,000 for fiscal year 2025; and

"(5) $49,000,000 for fiscal year 2026.".

(b) Conforming Amendments.—

(1) Section 2202(e)(1) of the Homeland Security Act of 2002 (6 U.S.C. 652(e)(1)) is amended by adding at the end the following:

"(S) To identify the technologies within the area of responsibility of the Critical Technology Security Centers as described in section 322 that are vital to national critical functions.".

(2) The table of contents in section 1(b) of the Homeland Security Act of 2002 (Public Law 107–296; 116 Stat. 2135) is amended by inserting after the item relating to section 321 the following:

"Sec.322.Critical Technology Security Centers.".