

Congress of the United States
Washington, DC 20515

June 6, 2025

The Honorable Gene Dodaro
Comptroller General of the United States
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Dodaro:

As the Government Accountability Office has reported for decades, cybersecurity remains one of the greatest challenges facing our nation. As we have become more reliant on technology and digital infrastructure, the number of discovered vulnerabilities has exponentially increased. Every day, our citizens, our critical infrastructure operators, and our federal, state, and local governments have to mitigate these vulnerabilities and defend against hundreds of thousands of potential cyberattacks. These come from criminals who take advantage of vulnerable people; foreign actors who threaten our critical infrastructure, and hackers who try to destabilize American businesses.

In response to these persistent threats, the Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA) has funded an initiative known as the Common Vulnerabilities and Exposures (CVE) program. This 25-year-old program leverages a broad community of cybersecurity stakeholders to publish standardized information about known cybersecurity vulnerabilities. This public-private partnership feeds into the National Institute of Standards and Technology's (NIST) National Vulnerability Database (NVD), the U.S. government's repository of standards-based vulnerability management data. NIST scientists assign severity scores to CVE vulnerabilities and ensure the information is usable by the community at large. Together, these programs underpin how organizations across the world mitigate vulnerabilities that could otherwise be exploited by malicious actors and carry out their broader cybersecurity programs.

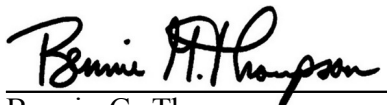
Both the CVE program and the NVD program have faced significant challenges in recent years. In early 2024, funding challenges at NIST resulted in a backlog of thousands of vulnerabilities in the NVD, a backlog that persists to this day. Further, a recent near-lapse of CISA's contract supporting the CVE program brought to light the security community's reliance on this program and the need to ensure its continuity. Given the programs' important role in ensuring our nation's cybersecurity, we request that the Government Accountability Office conduct a study of the federal programs designed to support vulnerability management for discovered vulnerabilities and weaknesses in information technology systems. Specifically, we ask that your office assess the efficiency and effectiveness of:

1. the NIST programs that support the creation and publication of standards-based vulnerability management data, including NVD;

2. the CVE program, including DHS's role in supporting CVE; and
3. Additionally, we ask that you assess the degree to which government and non-government entities rely on the NVD and CVE program.

Thank you for your attention to this matter. If you have any questions, please contact Alan McQuinn at (202) 225-6375 and Moira Bergin at (202) 226-2616.

Sincerely,



Bennie G. Thompson
Ranking Member
House Committee on
Homeland Security



Zoe Lofgren
Ranking Member
House Committee on Science,
Space, and Technology

cc:

Rep. Mark Green, Chairman, House Committee on Homeland Security

Rep. Brian Babin, Chairman, House Committee on Science, Space, and Technology