



September 11, 2018

The Honorable Greg Walden
Chairman
The Honorable Frank Pallone
Ranking Member
Committee on Energy and Commerce
United States House of Representatives

The Honorable Gregg Harper
Chairman
The Honorable Diana Degette
Ranking Member
Subcommittee on Oversight and
Investigations
Committee on Energy and Commerce

The Honorable Marsha Blackburn
Chairman
The Honorable Michael Doyle
Ranking Member
Subcommittee on Communications and
Technology
Committee on Energy and Commerce

The Honorable Robert E. Latta
Chairman
The Honorable Jan Schakowsky
Ranking Member
Subcommittee on Digital Commerce and
Consumer Protection
Committee on Energy and Commerce

Dear Chairman Walden, Ranking Member Pallone, Chairman Harper, Ranking Member Degette, Chairman Blackburn, Ranking Member Doyle, Chairman Latta, and Ranking Member Schakowsky:

The Cyber Threat Alliance and the Cybersecurity Coalition, on behalf of our members, write to express our agreement with the conclusions and recommendations of the Committee's Aug. 27th letters to the Department of Homeland Security (DHS) and MITRE regarding the Common Vulnerabilities and Exposures (CVE) program.¹

CVE is a critical program for cybersecurity

The Committee's Aug. 27th letters noted the CVE program's importance, referring to it as "critical cyber infrastructure."² We concur with the Committee's assessment. The CVE program is foundational to many cybersecurity operations and it is used in a wide array of cybersecurity-related activities, products, and services. In addition to the value provided to the private sector, the CVE database also supports a wide array of academic researchers, nonprofit security organizations, and government agencies. CVE identifiers have become the standard means for identifying vulnerabilities in software, allowing users to quickly access information about a problem across multiple information sources. CVE is a valuable resource for risk assessment, threat intelligence and information sharing, vulnerability notification and mitigation, intrusion detection and response, patch management, penetration testing, firewall management, security and threat operation centers, the National Vulnerability Database, and more.

Indexing vulnerabilities in a standard and interoperable format is useful for security practitioners, security vendors, and security consumers. A common means for vulnerability identification such as CVE will only become more important over time with increased use of software and digital devices that inevitably carry vulnerabilities.

CVE funding should be stabilized and expanded

The Committee's Aug. 27th letters note the program is funded on a short-term contract model with widely fluctuating allocations and scheduling.³ We believe this approach is unacceptable. As a critical element to operational cyber defenses, the CVE program should have the resources needed to ensure effectiveness and continued evolution.

We encourage Congress to appropriately fund these critical components to our national cyber security and allocate the necessary funds to DHS for this purpose. However, even in the absence of newly appropriated funds, we agree with the Committee's

¹ Letters from the Hon. Greg Walden, Hon. Gregg Harper, Hon. Marsha Blackburn, Hon. Robert E. Latta, Committee on Energy and Commerce, U.S. House of Representatives, to MITRE Corp. and the U.S. Department of Homeland Security, Aug. 27, 2018, <https://energycommerce.house.gov/news/letter/letters-to-dhs-and-mitre-corporation-regarding-cve-program-recommendations/>.

² *Id.*, Pg. 1.

³ *Id.*, pg. 3.

recommendation that DHS should establish CVE as a dedicated Program, Project, or Activity (PPA) with a line item in DHS' annual budget.⁴ We also recommend that Congress provide DHS with sufficient reprogramming authority for this program to address unexpected requirements that emerge during the year of execution. Establishing the CVE program as a dedicated PPA at current levels would provide consistency of funding and scheduling needed to enable long-term planning, and further demonstrate DHS' commitment to the program. DHS might also consider adding the CVE program to the Future Years Homeland Security Program to plan resource allocation and strategic direction for the next five years.

Continual improvement

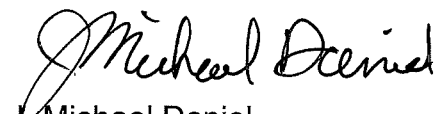
The CVE program faces challenges, in part because of the large and growing quantity and diversity of vulnerabilities. MITRE has been actively working with the CVE Board to design and implement improvements to the program. These improvements will assist the CVE program be more effective, efficient and able to scale to support the growing technology landscape. MITRE currently provides the CVE Board with a quarterly review of the status and metrics of the program. We concur with the Committee's conclusion that regular annual or biennial assessments of the program from DHS and MITRE can help determine where improvements can be made to ensure the program matches stakeholders' current and future needs.⁵ We would welcome the opportunity to assist with such an examination.

We commend the Committee for its proactive oversight, and we look forward to working with Congress, DHS, and MITRE to grow and improve the CVE program.

Sincerely,



Ari Schwartz
Coordinator, Cybersecurity Coalition



J. Michael Daniel
President and CEO, Cyber Threat Alliance

Cc:

The Honorable Kirstjen Nielsen, Secretary, U.S. Department of Homeland Security
Mr. Jason Providakes, President and Chief Executive Officer, MITRE Co

⁴ *Id.*, pg. 5.

⁵ *Id.*, pg. 6.