

**Congress of the United States**  
**Washington, DC 20515**

July 27, 2023

The Honorable Gene Dodaro  
Comptroller General  
U.S. Government Accountability Office  
441 G St. NW  
Washington, DC 20548

Dear Comptroller General Dodaro,

We write to request a GAO review of the Department of Homeland Security's (DHS) Port Security Grant Program (PSGP), including DHS's management of the program, its methodology for providing cybersecurity-related grants in accordance with seaport risks, and whether DHS's disbursement of grant funding has effectively kept pace with the growing scope of cybersecurity threats to U.S. seaport infrastructure. Findings from this review will help Congress determine whether DHS is identifying the most significant threats to U.S. seaport infrastructure and aligning grant resources to address those threats.

DHS administers the PSGP program through its component agency, the Federal Emergency Management Agency (FEMA), in coordination with the U.S. Coast Guard. The grants provide funding to state, local, and private-sector port facility operators to protect critical seaport infrastructure. FEMA's PSGP program announcement for FY 2023 identifies several priority areas for grant funding including support for increased maritime cybersecurity, port-wide maritime security risk management, and enhancing maritime domain awareness.<sup>1</sup> It further states that enhancing cybersecurity for U.S. seaports is among two areas that warrant the most concern based on the national risk profile for FY 2023.<sup>2</sup> We agree with this determination.

In particular, we are alarmed about the potential cybersecurity threat to designated strategic seaports in the United States that represent significant transportation and maritime hubs essential to the defense readiness, national security, and continuity of the economy of the United States. Recently, questions have been raised regarding the susceptibility of strategic seaports to cyber intrusions. In fact, a recent prominent example of the cybersecurity threat to our nation's strategic seaports has come to our attention. On May 24, 2023, the Cybersecurity and Infrastructure Security Agency, in conjunction with Federal partners, international cybersecurity authorities from the "Five Eyes" countries, and Microsoft,<sup>3</sup> issued a joint advisory warning critical infrastructure organizations about malicious activity by a state-sponsored cyber actor

---

<sup>1</sup> Federal Emergency Management Agency, *FY 2023 Port Security Grant Program Fact Sheet*, (Feb. 27, 2023), <https://www.fema.gov/grants/preparedness/port-security/fy-23-fact-sheet>

<sup>2</sup> *Id.*

<sup>3</sup> Microsoft Threat Intelligence, *Volt Typhoon targets US critical infrastructure with living-off-the-land techniques*, (May 24, 2023), <https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/>

The Honorable Gene Dodaro

July 27, 2023

Page 2

affiliated with the People’s Republic of China (PRC), known as “Volt Typhoon”.<sup>4</sup> According to press reports, Microsoft’s threat intelligence unit identified the malicious activity “while investigating intrusion activity impacting a U.S. port.”<sup>5</sup>

If these reports are correct, Volt Typhoon targeted our critical infrastructure in Guam and elsewhere in the United States, including the communications, transportation, and maritime sectors.<sup>6</sup> Guam hosts a significant U.S. military presence, which includes a designated strategic seaport shared by the U.S. military and the commercial seaport industry. This incident, in conjunction with recent statements from U.S. government officials<sup>7</sup>, makes a compelling case that cybersecurity concerns and the susceptibility of our strategic seaports are real and urgent.

To support further work of the committees on this issue, we request that GAO perform an assessment to include the following:

1. How DHS has identified and addressed challenges with administering the PSGP;
2. How DHS has determined the effectiveness of the PSGP, including determining the extent to which PSGP investments have reduced risks to U.S. ports, including cybersecurity risks;
3. How DHS has allocated PSGP funds to U.S. port industry stakeholders in accordance with risk, including cybersecurity risks and risks specific to U.S. designated strategic ports;
4. How port industry stakeholders operating at designated strategic seaports within the United States have used PSGP grant funding to replace equipment and technology manufactured by business entities affiliated with the PRC or the Chinese Communist Party (CCP) and their proxies; and
5. What improvements or policy options could be made to strengthen the PSGP, including the application and competitive review process, and the funding guidelines for applicants.

Thank you for your prompt attention to this important request. We respectfully request that this work be conducted as soon as possible.

Please contact Homeland Security Committee Majority staff at (202) 226-8417 and China Select Committee Majority staff at (202) 226-9678 with any questions about this request.

---

<sup>4</sup> Cybersecurity Advisory, Cybersecurity and Infrastructure Security Agency, *People’s Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection*, (May 24, 2023), <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a>

<sup>5</sup> David E. Sanger, *Chinese Malware Hits Systems on Guam. Is Taiwan the Real Target?*, New York Times, May 24, 2023, <https://www.nytimes.com/2023/05/24/us/politics/china-guam-malware-cyber-microsoft.html>

<sup>6</sup> *Id.* at 4

<sup>7</sup> Cybersecurity and Infrastructure Security Agency, CISA Director Easterly Remarks at Carnegie Mellon University (Feb. 27, 2023), <https://www.cisa.gov/cisa-director-easterly-remarks-carnegie-mellon-university>

The Honorable Gene Dodaro

July 27, 2023

Page 3

Sincerely,



---

Mark E. Green, M.D.  
Chairman  
Committee on Homeland Security



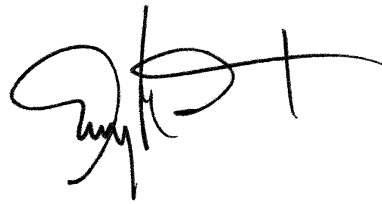
---

Mike Gallagher  
Chairman  
Select Committee on China



---

Carlos A. Gimenez  
Chairman  
Subcommittee on Transportation and  
Maritime Security



---

Anthony D'Esposito  
Chairman  
Subcommittee on Emergency  
Management and Technology