Congress of the United States
Washington, DC 20515

July 22, 2025

The Honorable Kristi Noem
Secretary
U.S. Department of Homeland Security
Washington, D.C. 20528

Dear Secretary Noem,

As the Department of Homeland Security (DHS) continues its critical mission to safeguard the American homeland, we are writing to raise concerns regarding the cybersecurity resilience of technologies used by U.S. Customs and Border Protection (CBP) at our Nation's borders.

CBP relies heavily on advanced Information Technology (IT), Internet of Things (IoT), Operational Technology (OT), and cloud platforms to execute its border security mission. These systems include unmanned aerial systems (UAS), biometric identification tools, autonomous surveillance towers and autonomous surveillance, land mobile radio communications, and the Border Enforcement Coordination Network (BECN). These tools have improved our border defenses, but they've also opened more digital doors for cyber adversaries—especially hostile nation-states and well-funded criminal organizations.

The BECN system plays a critical role in maintaining CBP's situational awareness and coordinating law enforcement activities along the border. A successful cyberattack on this or any related system could degrade surveillance, disrupt communication among operational units, or expose sensitive operational data to adversaries. These vulnerabilities must be addressed proactively.

Prior incidents underscore the urgency of these concerns. For example, the 2019 data breach during a CBP facial recognition pilot compromised sensitive biometric data, some of which was posted on the dark web. Last year, the CBP One mobile application was criticized for significant security vulnerabilities and lack of formal risk assessment, exposing critical infrastructure to exploitation and cyberattacks. Additionally, the increasing use of weaponized drones by transnational criminal organizations has introduced new, technology-driven threats to border security personnel and infrastructure. These examples illustrate the evolving and multifaceted nature of the cyber threat landscape facing our border security technologies

Given the strategic importance of these technologies and the significant risks posed if they are compromised by cyberattacks or other malicious activities, we respectfully request more information on the following:

The Department's current cybersecurity strategy and implementation plan to assess, prioritize, and mitigate cybersecurity vulnerabilities and misconfigurations across all Information

Technology, Operational Technology, and Internet of Things assets, identity management technologies, and cloud systems within the border security ecosystem, including:

- The funding currently allocated to protect these border security technologies from cyber attacks;
- The estimated funding level required to adequately protect these technologies from cyber attacks; and
- DHS's procurement plan to ensure that baseline cybersecurity protections are incorporated into existing and future acquisitions for border security technologies.

We must defend our borders not only from physical threats, but from the growing danger in cyberspace. Our adversaries are getting smarter, faster, and more aggressive. That means our defenses must be sharper, stronger, and always one step ahead.

Thank you for your leadership and dedication to this mission. We look forward to your response and to working together to secure our border security technologies from emerging threats.

Sincerely,

Morgan Luttrell
Member of Congress

Michael Guest
Member of Congress