MARK R. WARNER
VIRGINIA

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

United States Senate
WASHINGTON, DC 20510–4606

January 16, 2024

Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
1110 North Glebe Road
Arlington, VA 22201

Dear Director Easterly,

With less than 11 months before the 2024 U.S. Presidential Election, and the first primary already underway, I write with growing concern about the Administration's posture to combat foreign election threats. As the recently declassified Intelligence Community Assessment on *Foreign Threats to the 2022 US Elections* illustrates, a range of foreign adversaries continue to target our nation's democratic processes, with the goals of promoting greater social divisions, undermining confidence in electoral processes, and in some cases seeking to shape election outcomes. While the section of that Assessment that provides a prospective assessment for the 2024 elections remains classified, the IC has noted that foreign election influence activity tends to be elevated during presidential election years. Notwithstanding this persistent threat to our democracy, recent litigation by hyper-partisan actors has sought to stymie federal efforts to counter these threats.

The work of the Cybersecurity and Infrastructure Security Agency (CISA) has been pivotal in shoring up the nation's defenses since 2016. This includes not just CISA's vital work to assist state and local election administrators in protecting physical and technical aspects of election systems and electoral processes, but also CISA's efforts to serve as a nexus between the intelligence community, the private sector, and state and local institutions.

CISA's commitment to leading the federal government's engagement on physical security and cybersecurity ahead of each federal election is crucial. Since the designation of election infrastructure as critical infrastructure in 2017, CISA has led a collaborative effort to assist state and local governments, election officials, federal partners, and private sector partners in protecting election systems from cyber threats. The complex and often highly varied election processes and systems across the U.S. are markedly more secure today as a result of CISA's important efforts. However, recent elections have demonstrated the proclivity of foreign adversaries to pursue *blended* operations, which highlights the need to address election security holistically, encompassing both election interference[1] and election influence[2] threats. As the *2022*

[1] The Intelligence Community defines "election interference" to refer to "efforts aimed at degrading or disrupting a target's ability to hold elections, including by targeting the physical or technical aspects of an election. This includes cyber operations affecting a government's ability to register voters, cast and count ballots, or report results; cyber

US Elections ICA highlighted, for instance, Iran impersonated a U.S. violent extremist organization to send emails seeking to intimidate voters, as well as creating a website with death threats to US election officials. Similarly, in 2016 we saw Russia embrace hacking and dissemination operations (which included targeting political parties' networks and probing election systems), combined with social media-based election influence operations.[3]

In hearings the Senate Select Committee on Intelligence held in 2018, the Senate heard first-hand from senior social media executives how pivotal the Department of Homeland Security's election security efforts – in conjunction with those of the Federal Bureau of Investigation's Foreign Influence Task Force – have been.[4] Efforts by hyper-partisan litigants and media personalities to rewrite that history – and to falsely characterize these efforts, as part of an outlandish conspiracy theory, as somehow involving efforts by federal officials to suppress Americans' voices – should not intimidate your organization from maintaining this vital role.

The federal government has made substantial – if uneven – progress since being caught flat-footed in the face of sustained efforts by a foreign adversary to interfere in our democratic processes in 2016. Far from receding, these election threats have only *grown* – with a wider array of foreign malign actors, a larger number of social media platforms suitable for influence activity (and a combination of ownership and management changes reducing the private sector resources devoted to countering foreign election threats), and heightened incentives of many adversaries to shape election outcomes in pursuit of specific geopolitical objectives.

With the heightened possibility that the FBI may (through internal policy or court decision) be hamstrung in its ability to share threat information with impacted parties outside the federal government, it will be incumbent upon CISA to fill this vacuum – engaging and serving as an interlocutor between private sector entities, the intelligence community and law enforcement, and state and local officials.

Sincerely,

Mark R Warner

Mark R. Warner
United States Senator

---

operations degrading a campaign's ability to participate in an election; cyber or physical operations targeting election officials, poll workers, or polling places; and assassinations or military or security interventions affecting an election." *See* National Intelligence Council, "Foreign Threats to the 2022 US Elections," Intelligence Community Assessment (December 23, 2022) ("*2022 US Elections ICA*").

[2] The Intelligence Community defines "election influence" to refer to "covert or overt efforts by foreign governments, non-state actors, or their proxies, specifically intended, directly or indirectly, to affect an election. These activities can include efforts to sway public opinion; shape voter preferences for specific candidates or political parties; motivate or suppress specific voting blocs by raising contentious social issues; mislead voters about the time, manner, or place of voting; or undermine confidence in the results or political processes, regardless of whether these activities have a material impact on an election." *See 2022 US Elections ICA*.

[3] *See* Senate Select Committee on Intelligence, "Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume II," 116th Congress (November 10, 2020).

[4] Senate Select Committee on Intelligence, "Foreign Influence Operations' Use of Social Media Platforms," Open Hearing (September 5, 2018).