BENNIE G. THOMPSON, MISSISSIPPI
CHAIRMAN

JOHN KATKO, NEW YORK
RANKING MEMBER

One Hundred Seventeenth Congress
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

January 15, 2021

The Honorable Peter T. Gaynor
U.S. Department of Homeland Security
Washington, DC 20528

Dear Mr. Gaynor:

I am writing to urge the Department of Homeland Security (DHS) to do everything within its power to support Federal, State, and Local partners in securing State capitols and other targeted infrastructure against planned attacks, similar to the one carried out against the U.S. Capitol last week.

On January 6, the world watched as the U.S. Capitol was overrun by domestic terrorists, incited to violence by the words of the outgoing President. Law enforcement was overwhelmed, and lawmakers were forced into hiding from insurrectionists who sought to assassinate them. Multiple lives were lost, and many more were irreparably damaged. Once the smoke cleared, we learned more about the security failures that made this breach possible. Namely, a lack of preparation and coordination, slow and inept deployment of resources, and a seemingly willful blindness toward the intelligence gathered from online forums where these attacks were being planned. Indeed, the day before the attacks, the Federal Bureau of Investigation (FBI) reportedly issued a warning that extremists were traveling to D.C. to commit violence and "war." [1]

This week, the FBI issued a bulletin warning that "armed protests are being planned at all 50 state capitols from 16 January through at least 20 January, and at the U.S. Capitol from 17 January through 20 January." In another joint alert, DHS, the National Counterterrorism Center and the Justice Department reportedly warned that the Capitol breach would be a "significant driver of violence" ahead of the Inauguration, and that extremists "may exploit the aftermath of the [breach] by conducting attacks to destabilize and force a climactic conflict in the United States." These

---

[1] "FBI report warned of 'war' at Capitol, contradicting claims there was no indication of looming violence," WASHINGTON POST, Jan. 12, 2021, https://www.washingtonpost.com/national-security/capitol-riot-fbi intelligence/2021/01/12/30d12748-546b-11eb-a817-e5e7f8a406d6_story.html.

[2] "FBI warns of plans for nationwide armed protests next week," ASSOCIATED PRESS, Jan. 11, 2021, https://apnews.com/article/fbi-warns-armed-protests-next-week-ec75b26289166b4afd30c15b0dd2ded5.

[3] "F.B.I. Urges Police Chiefs Across U.S. to Be on High Alert for Threats," NEW YORK TIMES, Jan. 13, 2021, https://www.nytimes.com/2021/01/13/us/fbi-police-threats-inauguration.html.

attacks are reportedly being planned in online forums like Gab, Telegram, and even on mainstream sites like Facebook and Twitter.

Under Federal law, the Cybersecurity and Infrastructure Security Agency (CISA) is tasked with coordinating Federal efforts to secure all 16 sectors of critical infrastructure, including the Government Facilities sector, in preparing for and responding to elevated threats. To carry out this mission, CISA serves as a convener of coordinating bodies such as the Government Facilities Coordinating Council (GFCC) and the State, Local, Tribal, and Territorial (SLTT) Government Coordinating Council (SLTTGCC). CISA also provides guidance and other resources, upon request, to help critical infrastructure owners and operators harden their defenses against Improvised Explosive Devices (IEDs), active shooters, and vehicular attacks.

Relatedly, the Office of Intelligence and Analysis (I&A) is responsible for serving as a conduit for information sharing between the Intelligence Community and SLTT governments, leveraging a network of fusion centers. Through these relationships, I&A can share threat information critical to situational awareness for Federal and SLTT governments.

On January 6, we once again learned the importance of advanced planning and nimble coordination between branches of law enforcement and security forces. Warning signs were apparently missed, and resources did not deploy quickly enough to prevent destruction and loss of life. One can only imagine the consequences of this episode playing out at less-secured, less-resourced State capitols throughout the country.

This is precisely the convening and coordination role Congress envisioned CISA and I&A playing, but they must work proactively and directly with State and local partners. Disseminating paper guidance through email listservs is not sufficient to manage the threat we currently face. CISA, I&A, and other DHS components have expertise and resources that could help shore up defenses, as well as information sharing channels that can be used to rapidly share threat intelligence. As such, I urge CISA and I&A to swiftly bring the full weight of their authorities and resources to bear in securing SLTT infrastructure throughout the nation, with a focus on:

- Prioritizing outreach and assistance to government facilities and public officials most likely to be targeted by extremist groups, and assess whether the security resources available to those targeted entities and officials needs to be augmented;

- Convening the GFCC and SLTTGCC immediately, if these bodies have not yet been convened, to ensure that SLTT stakeholders understand the threat and the defensive actions they need to take;

- Making sure all information sharing channels are working seamlessly and threat intelligence is able to reach partners in law enforcement, fusion centers, and other SLTT stakeholders without delay;

- Providing regular security briefings, including classified briefings, to SLTT partners so that they have situational awareness about evolving threats;

- Producing intelligence assessments on potential threats to targeted infrastructure, such as State capitols, and sharing those products with Congressional partners where appropriate;

- Alerting the Committee to any resourcing issues within I&A or CISA that impede the ability to carry out these activities.

Ultimately the Department, through CISA and I&A, needs to understand the level and types of security resources available to SLTT partners, where those resources are deficient, and how additional forces can be deployed if necessary. While I appreciate efforts to bolster security in Washington, D.C. on and around Inauguration Day, we cannot turn a blind eye to the security and preparedness of our SLTT partners.

Thank you for your attention to this matter.

Sincerely,

BENNIE G. THOMPSON
Chairman

Cc: Mr. Brandon Wales, Acting Director, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security

Mr. Joseph B. Maher, Senior Official Performing the Duties of the Under Secretary, Office of Intelligence and Analysis, U.S. Department of Homeland Security