BOOST COUNTERTERRORISM CAPACITY AND DEFEND CRITICAL INFRASTRUCTURE

The national security of the U.S. requires that all individuals seeking entry to our country be properly and thoroughly vetted and screened, ensuring no individuals have a nexus to terrorism. Our Nation's ability to defend the homeland from potential terrorists is largely dependent upon our ability to prevent these individuals from entering the U.S. in the first place. Accomplishing this objective and expanding America's "virtual borders" within the framework of an evolving threat environment requires continued cooperation with our global and interagency partners, as well as enhanced and streamlined information sharing protocols.

During the previous administration, DHS greatly matured these processes through the opening of the National Vetting Center (NVC). The NVC allows agencies vetting individuals seeking entry into the U.S. to have a common framework for sharing and interpreting information, streamlining the process and ensuring that key information is not missed or "lost in translation" when communicated between different agencies and partners. The current administration's failure to continue this whole-of-government approach to counterterrorism has critically reversed many of those recent gains.

Over the past year, the Biden Administration has hampered the capabilities of CBP, one of the world's largest law enforcement organizations and the agency responsible for administering the NVC. The CBP must now constantly divert its limited resources to screen illegal aliens and care for unaccompanied alien children—a problem that is exacerbated by the current administration encouraging and incentivizing illegal immigration.

Counterterrorism efforts are a critical mission of CBP as it anticipates, detects, and intercepts threats before and at ports of entry. Key efforts include disrupting terrorist travel through passenger name record data, sharing watchlists of affiliated terrorists, and providing our allies with key tools such as the Automated Targeting System, which uses data for risk-based scenario assessments. These essential roles in our national security activities are less prioritized because of the border crisis.

Additionally, our Nation is currently seeing an inclination among some officials to significantly curtail federal, state, and local law enforcement collaboration. This collaboration is integral to our country's ability to identify and prevent terrorist attacks.

The Biden Administration's decision to halt participation in Immigration and Customs Enforcement (ICE) 287(g) program has also significantly decreased our internal capacity to protect the homeland. This highly successful collaborative program allows for the delegation of limited federal immigration authorities to participating state or local law enforcement entities. Moves among some officials to eliminate state or local participation within federal law enforcement task forces have had a similar effect.

The current approach places American citizens and communities at risk while compounding the risks to our digital and critical infrastructure—essential elements of America's national and economic security. Since the 9/11 attack, the threats against our homeland have evolved and become even more sophisticated. Vigilance in the face of these threats requires a willingness to commit to the principles of collaboration and information sharing that are essential to the identification and interdiction of terror attacks, whether physical or cyber in nature.

THE FACTS

- ★ Every day, DHS stops an average of 10 aliens on the terrorist watchlist from entering the U.S.
- ★ Today, nearly 200 Joint Terrorism Task Forces exist throughout the Nation.
- ★ Cyberattacks using malware spiked 358% in 2020, and cyberattacks using ransomware increased by 435%.

THE AMERICA FIRST AGENDA

At the federal level, support policies that:

- ★ Require cooperation with and participation in ICE's 287(g) program.
- ★ Appropriate funding for DHS's Homeland Security Grant Program to ensure continued robust support for the Nation's network of fusion centers.
- ★ Continue to expand America's "virtual borders" by enhancing our cooperative efforts with trusted global partners.
- ★ Facilitate partnership between the government and private industry to protect our cyber resources and critical infrastructure.
- ★ Direct the Intelligence Community to raise the priority of collecting, identifying, and disseminating information about cyberattacks from nation-state and non-state actors to private entities.

At the state level, support policies that:

- ★ Promote collaboration between state and local law enforcement with their federal counterparts through task force participation.
- ★ Develop Suspicious Activity Reporting protocols for state and local law enforcement agencies through participation in the Nationwide Suspicious Activity Reporting Initiative.

REFERENCES

2021 Mid-Year Cyber Threat Landscape Report, Deep Instinct (Feb. 2021).

Center for Homeland Security and Immigration Overview by Chad Wolf and John Zadrozny, America First Policy Institute (May 2021).

Costs of War, The Watson Institute for International and Public Affairs at Brown University (2021).

MYTH/FACT: Known and Suspected Terrorists/Special Interest Aliens,

U.S. Department of Homeland Security (Jan. 2019).

Protecting the Role of State and Local Law Enforcement in the Nation's Collective Effort to Prevent Terrorism by Scott Erickson, America First Policy Institute (Nov. 2021).

The Federal Bureau of Investigation and Terrorism Investigations, CRS Reports (Oct. 2021).

Transforming the U.S. Cyber Threat Partnership, The President's National Infrastructure Advisory Council (Dec. 2019).

Twenty Years After 9/11: Strong Federal, State, and Local Law Enforcement Collaboration Remains Essential in the Fight Against Terror – But It's Under Attack by Scott Erickson, America First Policy Institute (Nov. 2021).