STATES ON THE FRONTLINES OF COUNTERINTELLIGENCE

Wednesday, July 15, 2026

U.S. House of Representatives,

Permanent Select Committee on Intelligence,

Washington, D.C.

The committee met, pursuant to call, at 2:08 p.m., in Room HVC-210, Capitol Visitor Center, the Honorable Eric A. Crawford [chairman of the committee] presiding.

Present: Representatives Crawford, Kelly, Fitzpatrick, Scott, Hill, Crenshaw, Jackson, Steube, Tenney, Fallon, Himes, Carson, Krishnamoorthi, Bera, and Quigley.

Staff Present: Madison Aston, Professional Staff Member/Assistant Budget Director; Mandy Bowers, Subcommittee Staff Director; Griffin Decker, Staff Director; Meagan Devlin,Professional Staff Member; Matthew Johnson, Professional Staff Member; Lorelei Legg, Assistant Clerk/Staff Assistant; Lisa Major, Subcommittee Staff Director; Alice McIntosh, Professional Staff Member; Chase Sauvage, Professional Staff Member; Nicholas Richter, Clerk; Tara Westby, Professional Staff Member; Emily Ashbridge, Minority Associate Professional Staff Member; John Laufer, Minority Deputy General Counsel; Jeff Lowenstein, Minority Staff Director; Zachery Holland, System Administrator; and Kristin Jepson, Security Director.

The Chairman. Good afternoon, everyone. I call the committee to order.

Without objection, the chair may declare the committee in recess at any time. Before we begin today's hearing, I would like to provide a few important reminders. First, today's hearing is being broadcast live on the committee's YouTube channel. This open hearing will be conducted entirely on an unclassified basis. All participants are reminded to refrain from discussing classified or other sensitive information protected from public disclosure.

For this event, members will have 5 minutes with the witnesses. I would ask each of my colleagues to keep both your questions and witness answers within those allotted 5 minutes. Time permitting, we will conduct a second round, and any remaining questions will be submitted for the record. Additionally, in the same manner in which the House Permanent Select Committee on Intelligence has conducted itself in past hearings, I expect that we will continue to act in a bipartisan and respectful manner during today's event. I am confident all members can treat each of our witnesses today with due respect consistent with past practice.

Today's hearing is focused on understanding the counterintelligence fight facing our Nation from the lens of the States. Today we examine the role of State fusion centers in supporting counterintelligence. Further, we will also hear from our fellow State government officials on what they are doing to address expanding, pervasive, and entrenched foreign threats embedded across the whole of society. It is my pleasure to welcome our witnesses to today's hearing: President of the National Fusion Center Association and Northern California Regional Intelligence Director Mike Sena; Director of Alabama Fusion Center Jay Moseley; Senator Eliot Bostar, Nebraska's 29th District, from Lincoln; Representative Daniel Alvarez, Florida's 69th District, Hillsborough County; and Founder and CEO of State Armour, Michael Lucci.

The People's Republic of China has embraced a whole-of-society strategy that extends beyond traditional espionage. Beijing leverages legal investments, supply chains, research partnerships,

cyber intrusions, influence operations, and economic coercion to position itself for advantage long before any traditional conflict ever begins. This is not limited to espionage. Its preparation of the environment in our homeland is becoming an increasingly contested domain. The scale is staggering. Former Director Wray testified that the Federal Bureau of Investigation was opening a new China-related counterintelligence case every 12 hours, with over 5,000 active CI cases nationwide, half of which were tied to the Chinese Government. This also includes transnational repression reaching in our own communities.

In 2023, the FBI arrested two men running a secret Chinese ministry of public security police station out of a Manhattan office. One of more than 100 such outposts identified worldwide used to surveil and coerce dissidents living on American soil.

The PRC is so emboldened and comfortable operating in the U.S. that it established brick-and-mortar establishments to conduct repression of its critics within our borders. Iran and Russia too have escalated toward violence. Since 2022, the Justice Department has unsealed multiple State-sponsored assassination plots on U.S. soil, including Iranian schemes to kill a Presidential candidate and an Iranian-American journalist and a Russian-linked attempt against a CIA informant. These are not espionage in the traditional sense; they are foreign intelligence services treating American streets as battlespace. To win without firing a shot, the PRC for two decades has extended their penetration efforts beyond targeting Washington circles, endangering our States, our communities, and our universities, often gaining access to airspace and critical infrastructure. Much this activity unfolds in the gray zone, below the threshold of armed conflict or even criminal activity. Put simply, often their activities are legal and deliberately structured that way. Adversaries cloak these efforts as commercial hybrid threats, shell investments, front companies, and seemingly ordinary transactions blending State intent with private cover. This is why we are holding this open hearing, a format not often available in the Intelligence Committee. I am deeply concerned our next 9/11 level event has already been set in motion in the counterintelligence

domain. Our adversaries have prepositioned capabilities inside our infrastructure and telecommunications networks that could be activated at a time of their choosing. Campaigns like Volt Typhoon are not hypothetical. They are evidence of preparation happening today.

The American people need greater awareness of these threats to freedom, security, and our way of life if the Federal and State governments, the private sector and the people are to effectively counter these threats. Our panelists are vital to this because the first indicators will rarely appear in Washington. They may surface in a county zoning office, a university research partnership, a port authority, a sheriff's investigation of suspicious drone activity or, a fusion center connecting threads no single agency has seen alone.

State, local, and Tribal elements are indispensable partners. Our efforts must complement each other to deny adversaries the permissive, ambiguous operating environments they depend on. Last week, I held the committee's fourth counterintelligence related roundtable discussing at the State level in Huntsville, Alabama, preceded by roundtable events in Florida, Pennsylvania, and Arkansas. These events are part of the committee's ongoing efforts to bring the U.S. counterintelligence threat discussion to the State and local level.

The Federal Government cannot solve it alone. Winning this fight requires a true national effort. I thank our witnesses for their service and look forward to their testimony.

And, with that, I would like to yield to the distinguished ranking member, Mr. Himes, for his opening statement.

[The statement of The Chairman follows:]

******** COMMITTEE INSERT ********

Mr. Himes. Thank you, Mr. Chairman. And a big thank you to our witnesses for being here to share your expertise with us, in the same way that efforts to counter terrorism threats to the homeland are the shared responsibility of the Federal Government and State and local governments, efforts to identify and disrupt foreign intelligence threats to the United States, must be a joint Federal-State endeavor, with each partner bringing its unique understanding of the threat and its distinct legal authorities to the fight.

In a country as large and varied as ours, facing a complex array of intelligence threats from multiple countries, counterintelligence simply cannot be the exclusive province of the Department of Justice, the DHS, and then the Intelligence Community. The title of this hearing captures the fundamental reality that States truly operate on the front lines.

Two of our witnesses today represent State-operated federally supported fusion centers, part of a nationwide network of 80 fusion centers to bring Federal, State, and local officials together to identify and share information about and disrupt threats. The writ of these centers, which were stood up after 9/11, has since expanded beyond counterterrorism to cover counterintelligence.

I hope our fusion center witnesses will describe with as much precision as possible in this unclassified setting the types of foreign intelligence threats they are observing in their jurisdictions, how they share information about those threats with the Federal Government, and whether they are getting the Federal support that you need in the form of funding personnel and the timely passage of actionable intelligence.

Two of our other witnesses today are State legislators who are leading actors on the counterintelligence stage. I hope they will describe the legislation they have filed or enacted to address foreign intelligence threats within their States and the lessons they have learned from that experience.

Finally, I would ask all our witnesses to help us understand how they and we can strike the

right balance between the need to protect the American people from genuine foreign intelligence threats and the need to attract foreign direct investment to promote foreign trade, to encourage visits from international tourists, and, above all, to treat citizens, legal permanent residents and visitors fairly regardless of their ethnicity or national origin.

Thank you, Mr. Chairman. I yield back.

[The statement of Mr. Himes follows:]

******** COMMITTEE INSERT ********

The Chairman. I thank the ranking member for his comments.

And we are ready to move to witness statements. I ask that you keep your statements to under 4 minutes.

And now, Mr. Sena, I will start with you. You are recognized for 4 minutes.

STATEMENTS OF MICHAEL SENA, PRESIDENT, NATIONAL FUSION CENTER ASSOCIATION AND DIRECTOR, NORTHERN CALIFORNIA REGIONAL INTELLIGENCE CENTER; JAY MOSELEY, DIRECTOR, ALABAMA FUSION CENTER; ELIOT BOSTAR, SENATOR, 29TH DISTRICT OF THE NEBRASKA SENATE; DANIEL ALVAREZ, REPRESENTATIVE, 69TH DISTRICT OF THE FLORIDA HOUSE OF REPRESENTATIVES; AND MICHAEL LUCCI, FOUNDER AND CEO, STATE ARMOR.

STATEMENT OF MICHAEL SENA

Mr. Sena. Chairman Crawford, Ranking Member Himes, and members of the committee, thank you all for the opportunity to testify today on the counterintelligence threats facing our Nation at the State and local level.

My name is Mike Sena. I am at president of the National Fusion Center Association and also the executive director for the Northern California Regional Intelligence Center and the Northern California High Intensity Drug Trafficking Area.

Every day, over 3,200 personnel across 80 fusion centers work with Federal, State, local, Tribal, territorial, and private sector partners to detect threats, analyze intelligence, and support investigations, as well as coordinating operations.

We support a nationwide architecture that provides analysis and information sharing that complements Federal entities and information sharing partners, such as the FBI's counterintelligence task force, Joint Terrorism Task Force, the Homeland Security task forces, DHS' Office of Intelligence and Analysis, real-time crime centers, high-intensity drug trafficking areas, and regional information-sharing system.

Fusion centers provide something that is irreplaceable: the ability to fuse local operational context with Federal intelligence to ensure accurate information reaches the right people at the right

time.

The counterintelligence landscape has changed drastically, foreign intelligence services, most prominently the PRC, the People's Republic of China, along with Russia, Iran, and others are increasingly targeting State and local governments, Universities, critical infrastructure operators, and private industry. As a result, State and local partners are often the first to encounter involving espionage, cyber activity, foreign influence, supply chain compromise, and economic targeting. These threats are not theoretical. In California, a former Google engineer was recently convicted of economic espionage, stealing proprietary AI technology for the PRC, making it the first conviction involving AI-related espionage.

A former mayor in California admitted to secretly acting at the direction of the PRC, spreading propaganda and reporting back to the PRC on the activity and the outreach that that propaganda was doing. These cases underscore how foreign intelligence operators now actively exploit the gaps where Federal visibility is limited. States are building their own counterintelligence capabilities because current Federal information sharing mechanisms and classification barriers often prevent timely access to critical intelligence.

Key DHS and FBI systems remain disconnected and cannot support real-time multijurisdictional CI threat coordination. Delays in security clearances, inconsistent grant funding, and insufficient access to Federal systems reduce and impede operational readiness.

These gaps require modernization. Despite these challenges, State and local partners are rapidly adapting. The NFCA's new Counterintelligence Subcommittee brings together more than 110 members from 23 States to coordinate CI threat reporting, shared analysis and training. Embedding additional DHS Office of Intelligence and Analysis and FBI counterintelligence task force personnel can also significantly enhance coordination and information flow, something I have seen firsthand during San Francisco 2023 APEC summit, the 2026 Super Bowl, and currently during the FIFA World Cup games that we have been having in Santa Clara. Cyber and criminal networks are

also increasingly blending with CI threats -- from North Korean IT worker schemes, Chinese narcotics money laundering networks, to unauthorized drone activity over sensitive infrastructure.

To strengthen our national CI posture, I respectfully recommend establishing a national CI information-sharing framework that revitalizes the program manager for the information-sharing environment and the suspicious activity reporting standards for counterintelligence. Adding Federal CI personnel to fusion centers, improving clearance reciprocity and processing, ensuring predictable capabilities for funding and grant funding, enhancing our counterintelligence cyber integration, and also the FBI's administrative subpoena authorities to help us speed up the process of acquiring the data that we need, and strengthening training through the National Counterintelligence and Security Center.

Foreign intelligence services are adapting more quickly than we are. And we must leverage every available resource to fight this egregious threat to our Nation's security. States are responding, but they cannot and should not do this alone. Fusion centers can play a central role in connecting real-time local insights to Federal intelligence, but only if they have the authorities, access, training, and resources required.

Thank you for attention to this critical issue and to your continued partnership. I look forward to your questions and our shared work to strengthen America's counterintelligence posture. Thank you, sir.

[The statement of Mr. Sena follows:]

******** COMMITTEE INSERT ********

The Chairman. Thank you, Mr. Moseley.

STATEMENT OF JAY MOSELEY

Mr. Moseley. Thank you, Chairman Crawford, Ranking Member Himes, distinguished members of the committee. It's an honor to be appear before you today and am extra thank you to the chairman for coming down to Huntsville. That was a great event last week.

My name is Jay Moseley, and I serve as the director of the Alabama Fusion Center and Governor Kay Ivey's homeland security adviser. Thank you for the opportunity to discuss the increasingly important role State and local partners play in protecting our Nation from foreign intelligence threats.

Counterintelligence is no longer confined to Washington. Foreign intelligence threats increasingly target our States and communities, making State and local agencies a critical part of the Nation's counterintelligence enterprise.

When people think about counterintelligence, Alabama is probably not the first place that comes to mind, but it should be. Alabama is home to the Port of Mobile; Redstone Arsenal; Fort Rucker; the Air Force's fifth-generation fighter, the F-35; world-class universities; and a strong defense industrial base. These strategic assets make our State an attractive target for foreign intelligence services and demonstrate why States across the country are increasingly on the front lines of counterintelligence.

The Alabama Fusion Center is not an investigative agency. We don't duplicate the work of the FBI or the Intelligence Community. Our mission is simple: to get the right information to the right people at the right time so they can make informed decisions. But information sharing doesn't begin with technology; it begins with trust.

Technology helps to move information. Policies establish authorities, but relationships determine whether critical information is shared quickly enough to matter. Those relationships are built every day, not during a crisis. We invest in partnerships with the FBI, DHS, State and local law enforcement, the military, emergency management, critical infrastructure owners, and the private sector so that, when something unusual happens, people know who to call and trust that someone will answer.

One example that illustrates why those partnerships matter: An Alabama State capital employee observed an individual photographing building access points and other security features in a manner that appeared unusual. The information was shared with the Alabama Fusion Center and then with the FBI, DHS, and fusion centers across the country. What began as a single observation became part of a broader national picture demonstrating how timely reporting and trusted partnerships can help identify potential counterintelligence threats before vulnerabilities are exploited. This case and others included in my written testimony show that effective counterintelligence depends on identifying vulnerabilities early, sharing information quickly, and acting before an adversary can exploit them. Success is often measured not by arrest but by the threats that are prevented.

I also want to thank this committee for its bipartisan efforts to strengthen DHS Office of Intelligence and Analysis. Continued implementation of reforms that improve two-way information sharing, strengthen engagement with fusion centers, and expand field-based intelligence capabilities will make our Homeland Security enterprise even stronger.

As Congress considers the future of our Nation's counterintelligence enterprise, I respectfully offer two recommendations: First, continue strengthening the partnership between DHS I&A and the national network of fusion centers to improve two-way information sharing; second, sustain investments in fusion centers through Homeland Security grants, training, technology, and analytic capabilities, and counterintelligence awareness. Investing in these capabilities and the Federal,

State and local partnerships to support them is an investment in prevention. Foreign intelligence services exploit gaps between organizations and jurisdictions. Fusion centers help close those gaps by connecting information, people and capabilities across all levels of government, helping ensure threats are identified, shared, and addressed before they become crises.

Mr. Chairman, Ranking Member, and members of the committee, thank you again for the opportunity to be before you today. I look forward to your questions.

[The statement of Mr. Moseley follows:]

******** COMMITTEE INSERT ********

The Chairman. Thank you, sir. Senator Bostar.

STATEMENT OF ELIOT BOSTAR

Mr. Bostar. Chair Crawford, members of the committee, thank you for the opportunity to come before you today. Over the last 4 years, in partnership with national security experts and practitioners, Nebraska has passed a slate of laws to safeguard our State against foreign adversaries. We are filling gaps in America's broader security posture, and we believe all States, including Nebraska, must take additional action.

My work in Nebraska began when U.S. Strategic Command at Offutt Air Force Base reached out to my office with a clear warning: Huawei equipment had become pervasive near critical defense infrastructure, such as our nuclear missile silos, posing unacceptable risk to our national security.

The U.S. Government formally designated Huawei a national security threat in 2020, but years later its equipment was still in use and alarmingly being newly installed across Nebraska. We responded by introducing legislation in 2023 to pivot telecommunications companies from receiving State funds if they use or provide communications equipment designated a national security threat.

The law also cleared bureaucratic red tape for removing critical equipment. These commonsense reforms nonetheless triggered robust lobbying to keep the Beijing link technologies in use. It was our introduction into how foreign adversaries wield influence through their investments, including embedding themselves in trade and business associations, using these respected organizations as both a weapon and a shield. With each passage of legislation, the same pattern occurred. We would introduce a bill to address security threats. Foreign adversaries would exert their influence, often in unexpected ways that revealed something new about the use of

economic entanglement, political power, and coercion. We would come back the next session with legislation to address those newly identified tactics, and the cycle continued.

As we worked to remove Huawei equipment, we learned of another approach being used by the company to compromise our security. Critical infrastructure executives in Nebraska have been receiving special promotions for free Huawei smartphones, no strings attached. To the executives, it looked like marketing, but it functioned as access, placing adversary-owned hardware into the hands of the people running our grids, water systems, and communications. That episode caused us to take a harder look at Nebraska's procurement policies. We needed to close access to foreign adversaries. We addressed this with the passage of the Foreign Adversary Contracting and Prohibition Act, blocking companies controlled by foreign adversaries from State procurement involving communications technology, network systems and critical infrastructure.

In working to pass this law, we again experienced foreign adversaries' extensive lobbying power. Trade associations went to bat for our foreign adversaries, warning that the proposed commonsense guardrails would damage the economy and stifle innovation. So we had to demonstrate that such competitiveness concerns were a smokescreen. The issue of potential economic harm is important to address because it is frequently invoked as a talking to oppose efforts to strengthen security.

Our experience in Nebraska demonstrates that we are already facing economic harm that could grow substantially if we do nothing to disentangle our critical infrastructure and our economy from our adversaries. For example, as we work to pass legislation to shine a light on malign influence and lobbying activity, Smithfield, a company under foreign ownership, made veiled threats to State leaders that, if Nebraska moved forward with our transparency legislation, they could shut down food production in our State. With agriculture serving as the backbone of Nebraska's economy and Nebraska serving as the State that helps feed the Nation, that was a clear economic and security threat.

As our work advanced, additional coercive efforts came into view. Local officials reported direct outreach from CCP-linked actors. Victims of transnational repression began to speak up. Reporting emerged of an overseas service station operating in Omaha -- an unmistakable sign that foreign intelligence and coercive activity was occurring in our State.

Despite the very tactics utilized to prevent Nebraska from taking action, we have passed landmark legislation every year. These laws have positioned Nebraska as a leading State protecting our people from foreign adversaries. Even so, we are moving too slowly and have much more to do. This is even more true as we look across the Nation. While some States have taken serious action, others have done very little. And none of us have done enough. States have powered responsibilities to strengthen national security, but States are most effective in coordination with our national partners. That is why today I ask you to deepen the Federal Government's investment in sub national security work. Increased investment in our Nation's fusion centers and established more formalized systems of coordination with policymakers will help States across the country more quickly and effectively identify vulnerabilities, protect critical assets, and contribute fully and comprehensively to the defense of the American homeland.

Further, we must take a coordinated nationwide approach to decouple from foreign adversaries. We must strengthen our industries right here in the United States and build stronger partnerships with allies to reduce dependencies on foreign adversary nations. This can only happen with leadership from both our Federal and State governments.

With that, I thank you again for the opportunity to testify and look forward to your questions.

[The statement of Mr. Bostar follows:]

******** COMMITTEE INSERT ********

The Chairman. Thank you, Senator.

Representative Daniel Alvarez, good to see you. Thank you and you are recognized.

STATEMENT OF DANIEL ALVAREZ

Mr. Alvarez. Thank you, sir. Chairman Crawford, Ranking Member Himes, and distinguished members of the committee, thank you for the opportunity to testify today. My name is Danny Alvarez, and I represent District 69 in the Florida House of Representatives, covering Hillsborough County. I am a lawyer, which I hope you won't hold against me, a veteran of the United States Army, chair of the Florida House Criminal Justice Subcommittee, and vice chair of the Florida House Security and Threat Assessment Committee.

I am here today with a simple message: Florida will not wait for the Federal Government to defend our people, period. We respect our Federal partners more than you can understand. We value the coordination, but when threats are already touching our communities and State leaders are there, we have an obligation to act, and we will.

Counterintelligence is often discussed as if it only happens here in Washington inside Federal agencies or classified spaces, but the targets are not only in Washington. The targets are our in our States, and they are in our cities, our seaports, universities, our defense communities, water systems. They are in our agriculture fields. Every part of the State of Florida is vulnerable. And Florida is one of the clearest examples that we could give. Florida is not simply a large State. It is a national security State. We are home to major military installations, defense contractors, the Coast Guard operations, special operations equities, maritime infrastructure, aviation assets, and the space coast. Florida's defense economy is enormous. The threat is not theoretical for us.

Earlier this year, Federal authorities charged a Florida man in connection with alleged

attempted bombing at MacDill Air Force Base, an actual bomb at one of our bases. That incident is a stark reminder that Florida is not merely adjacent to national security; it is part of the target set our adversaries and hostile actors study.

Florida is also the gateway to America's future in space. Take Patrick Space Air Force Base, Cape Canaveral, the Eastern Range are all central to national security space launch operations, and that makes Florida an extremely attractive target, not just in the military domain but in the civilian, commercial, research, and space domain as well.

In plain terms, Florida is an exceptionally high-value target. Our adversaries know that, and we should know it as State lawmakers just the same. That is why the State rule matters.

In 2026, I introduced H.B. 945, a Statewide counterintelligence and counterterrorism unit bill. The bill would have required the Florida Department of Law Enforcement to establish and administer a Statewide capability focused on detecting, identifying, assessing, and countering threats from foreign adversaries, terrorist actors, insider threats, corporate threats, and hostile intelligence activity. The bill was not designed to duplicate Federal Government; it wasn't meant to be the Florida CIA. It was designed to close gaps that the States are already seeing.

Florida's openness is one of our greatest strengths. It is also the reason that we are targeted so much. We are a global State. We welcome investment, tourism, innovation, immigration. We want Florida to remain that way -- Florida to remain open, free, and prosperous. But openness without awareness becomes a vulnerability.

The answer, ladies and gentlemen, is not fear. The answer is disciplined security. It is not targeting the lawful speech or lawful association. The answer is identifying conduct, coordination, access, intent, foreign direction, exploitation, and threat-linked behavior. I need to be very clear on this point. State level counterintelligence cannot become a license to monitor Floridians for who they are, where they come from, who they love, what they believe, or what they lawfully say. That is not what I support, nor does anyone else I know. That is not what Florida should build.

A serious counterintelligence capability must protect civil liberties while protecting the State. Those are not competing missions. Those are both essential to the legitimacy of our cause, and they are the DNA that makes us the Unites States of the America.

The answer is also not a State acting alone. There is an answer in a Florida-State partnership, a Federal and State partnership that recognizes the States as the frontline censors. So that is why I believe Congress can act in five practical ways.

First, Congress should strengthen the flow of timely, useable counterintelligence information to State and local leaders. Not every threat briefing needs to be classified. States need more unclassified, controlled, and actionable information that can be shared with relevant team members.

Second, Congress should support State level training and best practices. If States are expected to help defend the homeland against foreign adversaries, then State and local officials need the training on what foreign intelligence activity looks like in the real world. That includes procurement risk, insider threat, cyber targeting, influence operations, transnational repression, research security, land-use vulnerabilities, and critical infrastructure access.

Third, Congress should help define the guardrails. States need to protect their people without infringing on constitutional rights. That means clear standards focused on behavior, threat activity, foreign direction and exploitation, not political viewpoint, religion, ethnicity, or lawful expression.

Fourth, Congress should encourage better integration between Federal agencies, State domestic security structures, and fusion centers. Florida does not need a disconnected intelligence bureaucracy. We need coordination that is timely, lawful, practical, and, most importantly, trusted.

And, finally, Congress should recognize that adversaries exploit the seams. They exploit the seams between us and you. They exploit the seams between the public and private sector, law enforcement and intelligence, between the economic development and national security, between our openness and our strategic negligence. Our response has to focus on closing the seams.

H.B. 945 unfortunately didn't become law that time, but I am not done. Florida will continue to work building the most proactive capability that protects our citizens, strengthens our public safety, and safeguards critical infrastructure while supporting our Federal partners in the fight together.

We will continue refining the model and improve the safeguards, but we will never pretend this threat is theoretical. America's adversaries are coordinated, patient, and strategic. Our response must be the same. The Federal Government has unique authorities, collection capabilities, and global reach. And States, they provide proximity, local visibility, and constitutional responsibility for public safety. We need both. The lesson I hope the committee takes from Florida is straightforward: State governments are no longer peripheral to national security; we are part of the front line.

Thank you for the opportunity, Mr. Chairman.

[The statement of Mr. Alvarez follows:]

******** COMMITTEE INSERT ********

The Chairman. Thank you, sir.

And, finally, Mr. Lucci.

STATEMENT OF MICHAEL LUCCI

Mr. Lucci. Thank you, chairman Crawford, Ranking Member Himes, and members of the committee. My name is Michael Lucci, I am the founder and CEO of State Armor. We work State by State to help enact protections for critical infrastructure, security measures for supply chains, and work to counter foreign influence campaigns.

I will point to three points to highlight the challenges and opportunities of counterintelligence at the State level. First, counterintelligence gaps exist in our Federal system because of the division of powers between the Federal Government and the States. Second, the CCP seeks to exploit these gaps. The infiltration at the State level is significant and cause for alarm. And, third, with your encouragement, the States can and should become 50 bulwarks of counterintelligence to close the gaps exploited by the CCP.

These gaps exist because we are a massive continental power, an open society, and we divide power between Federal and State level. Yet, Federal warnings consistently point to significant subnational threats and the need for State action.

The Jamestown Foundation in 2019 pointed to China pivoting towards the States. Secretary Pompeo in 2020 warned all Governors that they are being targeted by the CCP. President Biden in 2022 put out a memo describing how subnational influence operations affect the States. And then Biden, in 2024, warned all Governors that their watering structure was being targeted by cyber attacks.

President Trump issued an executive order last year stating that States need to play a greater

role in national resilience. And then the New York Times reported last year how the Chinese consulate in New York weaponizes 50 community organizations to work against candidates in New York who are against the CCP.

The infiltration is a serious cause for concern. For example, Laughlin Air Force Base, Grand Forks Air Force Base, Whiteman Air Force Base, and Barksdale Air Force Base were all found to have Chinese penetration near the bases. And that was all mitigated by State and local authorities.

Threats to critical infrastructure are even broader. The Washington Post has reported on Chinese-made solar inverters that could be remotely sabotaged spread across the country, particularly in my State of Texas. And, furthermore, in Texas, the Senate Intelligence Committee has reported on Chinese cryptocurrency miners that could be remotely sabotaged to cause oscillations across power grids. That is just one sector of critical infrastructure. Universities are also targeted, and so are State governments and legislatures themselves. Chinese and American businesses lobby in State legislatures for China's interest. United front style pressure campaigns flood State houses when States do engage in counterintelligence work.

We think that the solution is for States to be empowered to be the first line of defense to leverage our federalist system and transform States into these bulwarks of counterintelligence.

A couple ideas, regular messaging from you all place a tremendous role in State activities. I could tell you about just one statement by Congressman Krishnamoorthi that led to a series of protective State actions. Federal-State partnerships with Federal guidance to use State powers to amplify your efforts; increased State lawmaker involvement in Homeland Security war games so they could understand how these things might play out; encouragement for States to match Federal efforts, especially when that encouragement could be made on a bipartisan basis; and ongoing education to recognize and counter both united front influence campaigns and transnational oppression would be hugely valuable to State and local law enforcement.

In conclusion, we believe that America's best response to CCP is to turn our decentralized

system into a strategic asset. With increased Federal guidance and encouragement, States will discover and solve problems in their backyards before Washington, D.C., even knows about them. I have seen it happen repeatedly.

Furthermore, these novel State solutions can then become a consideration for you all to adopt as national policies.

Thank you for the opportunity to testify. I look forward to your questions.

[The statement of Mr. Lucci follows:]

******** COMMITTEE INSERT ********

The Chairman. Thank you, Mr. Lucci.

And I now recognize Vice Chairman Kelly for questions.

Mr. Kelly. Mississippi has a significant military and national security footprint, including Camp Shelby, critical work conducted at Stennis Space Center, defense contractors all over the State. As foreign adversaries increasingly operate below the threshold of traditional conflict, State and local partners must be able to recognize suspicious activity, connect seemingly isolated incidents, and quickly share that information with military law enforcement and Intelligence Community partners.

Mr. Sena, how closely do fusion centers work with military installations, Army CID, NCIS, Air Force OSI to integrate and correlate suspicious activity reporting involving military bases and other sensitive facilities?

Mr. Sena. Thank you for the question, sir. The National Network of Fusion Centers' primary job is to do that outreach coordination collaboration. So having those partners that are in those installations connected to our network as well as understanding what our suspicious activity reporting models are and getting that information. There have been issues in the past where there have been gaps. Unfortunately, sometimes it is based on the personalities of the folks in the fusion center, the personalities on the bases, but the goal being is that we all have to be looking out and looking well beyond the perimeter of the base, the installations, the locations that we are trying to protect. I bring to light the use of drones and drones that are constantly going over -- going near our military installations. Those don't start necessarily right near the bases. So we have got to have the ability for real-time information sharing between those installations and folks on the outside. So there is that collaboration. There is that coordination. Is that the level that I would like it to be? No. But I think that is something that we should drive to achieve because they are a prime target for our adversaries.

Mr. Kelly. Yeah, I think that is one area we have to look at real closely is drones, whether

personal, whether a 12-year-old kid, or an adult or a foreign agent, I think that there need to be either fines or criminal penalties depending on intent and capabilities of those when they fly over any military or sensitive facility. And, if we don't change the laws on this, we are going to have a catastrophe happen. And there needs to be criminal or penalties of some sort -- it can by fines. If a 12-year-old accidently flies it over Camp Shelby, he probably should not go to jail, he or she. But they absolutely, their parents should be fined for allowing them to do that.

Saying that, are there any classification, authority, technology, staffing issues that we can help with for our fusion centers that will shore up some of the shortfalls that we have?

Mr. Sena. Absolutely, sir. And, you know, a primary issue is the training, education. And we had a huge kind of push coming up to World Cup to get people trained, going to Alabama to get the training to be able to respond to that counter-UAS threat. But I also have to say that there have been major issues with that regarding the resources, the acquisition of the technology, the deployment of the personnel. And I am actually going to defer to my partner from Alabama to talk a little bit about some of things that he is seeing on the ground.

Mr. Moseley. Thank you, sir. Yes, some of the things we are seeing on the ground when it comes to the counter-UAS training there is only one place for it; that is the schoolhouse in Redstone. Although that is great, we think there should be more training, more ability to get that training. So that is one place where you could probably help out. And I don't know the answer to that. But we need more training and more availability to the training.

I think the other piece is the ability to bring a drone down safely. I know we are working towards that, but there is a big limit there on what you can actually do. We can detect them, but, you know, the challenge there is to bring it down safely. So I think that is a couple of places where we could work on that.

Mr. Kelly. It is not too long ago where we had an air balloon transit the entirety of the United States, including many sensitive facilities, and we didn't take it down when we had an

opportunity. And then we couldn't down it down at other locations because of collateral damage that might have occurred. But I am just telling you we have to really look at the laws and these drones. Most times it is not nefarious intent. It is just a kid out there playing with a drone or an adult out there playing with a drone, but there have to be consequences when they over fly sensitive areas of the United States, regardless of intent. Now, they don't all need to be criminal. I am a former district attorney. So I forgive you for being a lawyer. I was a good lawyer. But, that being said, we need to really look at, and I think it is going to take a lot of local input because we don't have the database of knowing what exactly, and Mississippi isn't much different than Washington, D.C., and Chicago, Illinois, or western California or Oregon. And so we really have to have input from the States to make sure that we have laws that comply, but also protect us.

And, with that, Mr. Chairman, I yield back.

The Chairman. The gentleman yields.

Ranking Member Himes.

Mr. Himes. Thank you, Mr. Chairman.

Mr. Moseley, I want to start with you. You said something that intrigued me, which was that we need to -- because I am always looking, by the way, for the oversight hearing. It is hard to get what are we doing wrong. But you said we should strengthen the partnership with FBI and with A&I in particular. So put some specificity on that. Are you not getting the information you need? Tell us how we can fix that.

Mr. Moseley. Sure, I love talking about that. So are we getting what we need? Yes. Bottom line, yes, we are getting what we need. I will start with the FBI. We have got two field divisions in Alabama. I will start with Alabama and work our way out. So, in Alabama, very solid relationships with the FBI, and it goes deep. It goes to the intel component all the way up to our SACs, a lot of engagement, a lot of discussions, a lot of meetings, working groups, Red Cell exercises, tabletop exercises, joint products. So we are getting it where we need, but it is not consistent

across all 80 fusion centers. So that is where I think you can play a part in that is trying to work on the consistency. What I received in Alabama, Virginia should receive it; California should receive it, all --

Mr. Himes. So how do we -- Mr. Sena is nodding there, not unexpectedly. So how do we -- how do we -- do we survey all 80 -- as a committee, do we survey all 80 fusion centers? How do we fix that?

Mr. Sena. Well, and there was a process that we developed in 2017 enhanced engagement initiative to kind of calculate where do we have gaps. And it has gone through a number of iterations on the FBI side. But I really think that there should be a focus on that. You know, developing a report card that says, are we getting the -- and it goes both ways. You know, are the State and locals and the fusion center and the partners that we have doing the contribution that we need to the FBI to complete what they need to do, but are we also getting the things that we need. That information sharing, there is a lot of silos, unfortunately. Here we are 25 years -- getting close to 25 years after 9/11, and we still haven't resolved this issue between DHS and FBI and the information sharing. But, when it comes to that information sharing, if people don't have the right clearances, they don't have the right access.

Mr. Himes. Would every fusion center -- would every fusion center have an individual with a TS/SCI, or is that rare?

Mr. Sena. Well, I do have to say DHS manages the fusion center clearances, which are at the secret level, and then, at request, at the top secret level. But, in my center itself, I have had to go to the FBI and say, "Hey, I need get all of these folks TS and, in some cases, SCI clearance." And many of them are getting assigned to support, you know, the JTTF support, our counterintelligence task force, but it is an ad hoc. It is not consistent where people are getting TS and SCI access, where most of the counterintel information lies.

Mr. Himes. Okay, speaking of information sharing, Mr. Lucci, you gave an example that was

of some interest to this committee, these bitcoin mining centers. It was of particular interest to the chairman. I have to be oblique about it, but a Federal agency did a fairly indepth investigation of that and arrived at a fairly firm conclusion. It sounds like you have not seen that.

Mr. Lucci. Congressman, what I have seen is from the Senate Intelligence Community in a report last year that described the company BITMAIN as a threat.

Mr. Himes. No, no. I am referring to an investigative agency that did some work here. And it sounds like you haven't seen that report.

Mr. Lucci. I have not read that report.

Mr. Himes. Okay, I mean, that is an example of -- because you are spending time thinking about this. That is an example of a failure, a very clear example of a failure to share information. So what can we do? What can we do to make classified -- I understand the challenges, but what can we do to make it? You don't even know what you don't know, right?

Mr. Lucci. Right.

Mr. Himes. Because -- and I am being oblique about this, but what is the solution to that?

Mr. Lucci. Congressman, an example that I gave in my longer testimony, in terms of targeting State lawmakers, if you just have iterative information sharing, maybe through a web portal about whatever the unclassified findings are on this topic or otherwise -- Congressman Krishnamoorthi one time said one statement about routers that are dangerous that led to a whole series of positive State actions to counter those threats. So just having an information portal that is open source of things that are already happening that you want States to know about would be extremely valuable.

Mr. Himes. Great suggestion. Thank you. That is exactly what I am looking for.

One last question because I don't have a lot of time left. But the flip side of "if you see something, say something" and it really mobilizing here is that we are going to see an analogy to what we saw in the CT world, right, where Sikhs are getting approached because they may be

al-Qa'ida or whatever; civil liberties are really important. So tell me, maybe starting with you, Mr. Sena, what are we doing to make sure that overly enthusiastic law enforcement or citizens aren't approaching every individual with Asian features with a camera?

Mr. Sena. Absolutely. And that is a huge part of what we do as far as that suspicious activity reporting. A core element of that is privacy, civil rights, and civil liberties. So they have to have that training that not only says what do you look for, but what do you have to balance as far as those key indicators. And photography, a prime example, taking photographs is not illegal. But it is the context; it is how it is done. And you have to approach it in a certain way when you are doing your followup and your investigation. You don't want --

Mr. Himes. Is this training you are referring to, is that broadly mandated to local law enforcement?

Mr. Sena. I will tell you it is not. And we have started to get it in some areas and actual police academies and other locations where people are being trained. But it is not broadly disseminated to everyone out. You know, a number of centers are relying on Homeland Security grant funds. But we have seen, even this last cycle, funds not getting to where they need to be and some centers actually not getting their funding at all. So this becomes problematic when you don't have the funding to do the training, but that is part of the training that we have to get out there is that, how do we protect the rights that Americans have in this country?

Mr. Himes. Yes, I appreciate that and very much appreciate the testimony of our sibling legislators. That is an area where I think we can probably work together. We have got to make sure that we are not creating unfriendly communities just because we are attuned to the threat. Thank you.

I yield back.

The Chairman. Thank you.

I am going to recognize myself real quick here. Representative, you -- I know that, at a

National Fusion Center Association event recently, FBI Deputy Director Wray spoke about expanding the Bureau's support for fusion centers. Are you seeing that? Any meaningful changes there -- Federal engagement, resources, information sharing -- since that commitment?

Mr. Sena. I have to say that, you know, the support they provide is very generous, but I have not seen an increase since those comments were made towards a number of these efforts. And, as I said, oftentimes when we rely on the coordination between fusion center directors and their special agents in charge or in those areas where they have assistant directors, it is a case-by-case basis. We have some that is phenomenal, and we have some where they may not communicate as well as we would like. But the conversation has to go both ways. And I can tell you, in my jurisdiction where I work out of San Francisco, I am in constant communication with special agent in charge, with the ASACs, multiple times a day, but it is not always that way.

The other part of that is the deployment of personnel. We need, you know, those FBI, you know, points in every center in our country. And that is not always the case where we have the people that are there co-located, working together. Without the FBI connectivity there full time, you don't have connectivity.

The Chairman. I am got questions for all of you, but I have only got 5 minutes so I am going to go to Mr. Lucci on this, because you have written extensively about reducing America's strategic vulnerabilities as applies to PRC. And so, if you were asked with, you know, or tasked with rather designing a long-term national counterintelligence strategy, one that may be analogous to George Tenet's strategy of containment, what would be the central organizing principle of that? And how would success be measured over the next decade?

Mr. Lucci. Congressman, I will speak mostly of a State approach, because that is how I come at these problems is, one, there is just lack of information and lack of awareness of whether State leaders are -- whether Federal leaders want State leaders to act to counter these threats. So step one is establishing that you want them to act and to start information flows of threats there in their

State. But more importantly is tools and resources that they can use to investigate say a suspicious purchase near a military base or a critical infrastructure. We see those purchases happen, but it is unclear who has the real knowledge of what is behind that. I know sometimes you go to a fusion center; sometimes private firms.

Third, I would say there should be a disentanglement of our universities from theirs at least to some extent. It should be noted that the Chinese Communist Party's plan to take over the nationalists in their civil war of a hundred years ago first began by infiltrating their universities in very specific ways. That is happening here. I mean, the exact same playbook that they did domestically to the nationalists is happening with our universities here as well. I think that that is a major access point into our State institutions is infiltration of our university system.

And, last, there needs to be much more transparency about united front operators. States don't know what this activity is really. I mean, they just see the tail end of it in State houses all the time. Those would be very important components from a State perspective to counter these PRC-influenced campaigns.

The Chairman. Thank you. I am going to -- I had posited that the National Guard could actually be leveraged from the perspective of domain awareness, because domain awareness is critical to counterintelligence. The National Guard is present in every State, but they have that built-in connectivity to the Federal Government through those relationships that exist in the military.

So my theory is that maybe we could leverage National Guard assets as a contributor, in fact, a pretty important contributor in the CI fight. I am going to throw that out there and let anyone of you address that and if you see the value in that operation. Mr. Moseley.

Mr. Moseley. Yes, just real quick, I will say the provost marshal is where we -- I think it is a great place to start. Every State has got a provost marshal. They have got their direct connectivity, like you said. We have got a good relationship with ours, but you also have turnover. But, as long as there is a continuous turnover where they are briefing the next one, I think that is the

good place to start, and that is a good idea you have got.

Mr. Sena. And, as a person who has 22 National Guard members assigned to a counter drug task force who do a phenomenal job -- the Guard has got exponential capabilities and resources that should be taken advantage of. Very smart folks out there that have experience and training and those that have the CI training, getting them engaged to help support absolutely as much as we can because our adversary is attacking us every day, every way that they can. And we need to leverage every single resource that we have, including the National Guard.

The Chairman. Okay.

Mr. Alvarez. Thank you, sir. The Florida National Guard actively right now operates 90 days on average out of the year. That is their deployment route and scheduling. And so we have done that in other mission sets so the CI one is a natural extension of a capability set that they have. And they would get into that fight if we gave them the mission set. And I think it is a brilliant idea because we have trained them. We have paid for it, and they are itching to use the knowledge to defend the homeland. So let's get them in the fight.

The Chairman. Outstanding.

Senator.

Mr. Bostar. Thank you for that question. I think absolutely the National Guard is an appropriate avenue to pursue for this work. But one thing I will add is the National Guard lives in the executive branch; the fusion centers live in executive branch. One thing that we need to be deliberate about is applying that connectivity between State executive branch government entities and the legislative branch, because the policy component is so important and is, I fear, too often overlooked in how we can move the ball forward in the counterintelligence space and protecting our residents.

The Chairman. Gotcha, thank you.

Mr. Carson.

Mr. Carson. Thank you, Chairman.

Fusion centers rely on DHS Office of Intelligence and Analysis for Federal personnel and timely threat information. But the administration is now proposing cuts and a major reorg of that office. My friend Jim Himes is tired of hearing me say this, but I am still the only Member of Congress to go have served in a fusion center. And I love him for it. He is so patient. He is so patient. But I am concerned that these changes could weaken the system that our State and local partners rely on.

Mr. Sena, Mr. Moseley, would these proposed changes -- or anybody for that matter, would these proposed changes make it harder for you detect and essentially stop foreign threats?

Mr. Sena. Yes, absolutely. And, you know, our partners at DHS I&A are the only branch within the executive government that has that responsibility for coordinating with State, local, Tribal and territorial partners. They are not investigative agencies. They are there to do analysis to support intelligence. And, if we lost those bodies, you know -- the field, I know that they want to strengthen the field, but we need a backbone at headquarters. You know, you can't send out a whole bunch of soldiers in the field without command and supply chain backing them up. It will fail.

And I have got to tell you every place needs more I&A personnel that are supporting them. And we still have got promises from DHS I&A that we have vacancies in places across the country where they don't have an I&A person, but they said they are going to get those people out there by September. I am going to hold them to it, but we need more people, not less.

Mr. Carson. Yes, sir.

Yes, sir, Senator.

Mr. Alvarez. Thank you, Mr. Carson.

The fusion centers are the bones of the fight. We need to flesh out the muscle by bringing in local agents, deputies, police, all sorts of State and law enforcement agencies to flesh out the bones. We shouldn't be cutting it in any way; we should be enhancing it. So, when originally it was a counter terror threat like we set it up in 9/11 -- and it is an incredible model. The further we

get from 9/11, we are, like, okay, now what? But the counterintelligence fight, we are just getting in it. If you cut out the skeleton, I now have to rebuild that at a State level, and I don't have, number one, the authorities, right, when it comes to intelligence. I have to have a law enforcement precept to go in there, right. We have to have some investigatory reason to go under a law enforcement crime predicate. So, if you do that, you are crippling my ability as a State. But I also believe you are crippling the Nation because we have got this incredible asset; we have built it over 25 years. Even if the mission set changes, let's morph it into the CID idea now because the level and the threat has changed. So cutting it would be a really bad idea.

I would argue that we need to make it more robust. I need more of them. I need even more analysts. I need -- crime doesn't know borders, sir, and neither does the CI threat. So we need more of it.

Mr. Carson. When I served, we had a SCIF that was overseen by Bureau, by the FBI, but that is not universal. Not all fusion centers have SCIFs. Might that be problematic going into the future?

Mr. Sena. Absolutely.

Mr. Moseley. Yeah, I will just real quick, yes, it would be. And you are right: All don't have it, or all have an outdated one. We have got a really nice one, but it was built by DHS, and we are lucky do have it, but they don't all have it.

Your I&A question, so like we need more out in the field. We have had a vacancy in our shop for going on a year now. And I know they are trying to get it filled, and they say they will, and I believe them that they will. But, when you have only got one in the fusion center and that person is retired, on leave, they are gone, or they are deployed to the southwest border, whatever it is, we are vacant.

And, like Director Sena said, that is the only agency statutorily required to share classified information with State and local. Out of the whole IC, that is the only one. So we can't cut it.

We need it in the field.

Mr. Carson. Yes, sir.

Thank you, Chairman. I yield back.

The Chairman. Thank you, Mr. Carson.

Mr. Scott.

Mr. Scott. Thank you, Mr. Chairman.

Representative Alvarez, I represent I-75, from the Georgia-Florida line to all the way just north of Macon. And we had a stop in Houston County. Our Houston County sheriff's office picked up a bunch of cash from a stop, duly accounted sheriff's office picked up a bunch of cash from a stop. The Alachua County Florida office, sheriff's office, all on I-75, hundreds of thousands of dollars bundled the exact same way. And ends up these are Ukrainian nationals transporting what ended up being almost $1 million worth of cash all on I-75. I say that to get back to the point that our local and State law enforcement, there are a whole lot of them, and they are the first to see what is happening. And I am glad you are moving ahead and not waiting on the Federal Government in Florida. My wife is from Miami. You have got Orlando. I mean, Florida is truly -- you have got MacDill Air Force Base right outside of where you live.

Mr. Alvarez. Yes, sir.

Mr. Scott. I will add to what the ranking member said about the crypto mining. I understand there is crypto mining going on just outside of MacDill Air Force Base. Why we allow that in the United States of America is baffling to me.

By the way, to American citizens, the computers come from China. China doesn't allow them to operate in China, but they send them to the United States of America, and then they operate them right next to our military bases. It is ridiculous that we allow this in our country.

But my question for you, I have been to the fusion center in Miami, which was almost all local. I went down there with the FIFA to look at them and how they were handling security. If you were

sitting in our shoes and you are paying attention to this from the State level, what could we do today that would help you accomplish what you are trying to do at the State level for the State of Florida? What is the number one, number two, number three things we could do to help you?

RPTR DEAN

EDTR HOFSTAD

[3:04 p.m.]

Mr. Alvarez. Well, the first thing, sir, I think, is information. We are in the nascent part of a State involvement. We are waking up to the fact that we should have been involved 30 years ago. It didn't just show up; we all know that. The Feds, you know, have been dealing with it.

But let's use the example that you said right there of your local deputy. That local deputy pulls over the car. If he or she isn't trained in some of the factors of what they are looking for, they just see someone with a lot of money. They call their sergeant. The sergeant says, "Well, is there any predicate of a crime here?" "No, there's just a lot of money," and they just let it go.

Even if they would have just put that information up to their local fusion center, up their chain of command, that would have helped us out start connecting the dots that doesn't know a border, right? The crime didn't know a border.

But we are not even there yet, right? So, in Hillsborough County, for example, I have 1,500 deputies. I have another 1,000 in the city of Tampa, a couple periphery police departments. If I could get all of those folks CI-trained in some sort of information, that would be key.

The other part, sir, that we look over a lot of times is engaging our business community. So our business folks, a lot of times they will start to get penetrations in their business and they don't have any idea.

You might be a lead manufacturer in Lake County, Florida, and the next thing you know, you have a lot of inquiries as to lead and why you need lead. And, well, we know we use lead in ships. And all of a sudden --

Mr. Scott. Uh-huh.

Mr. Alvarez. -- why were you asking for this big purchase of lead?

So, if we had taught these people to be aware of what to look for for these inquiries that

come in, they become soldiers in the field helping us roll up information as well.

So, sir, first off is training and information.

Second off is information-sharing. So we know that silos kill, right? Silos kill.

Mr. Scott. A hundred percent.

Mr. Alvarez. They hurt the Fed, they hurt the State, they hurt the county. When we don't share information and we act like it is just about us, that is the worst thing possible. So we have to get rid of barriers.

And the other thing, sir -- and I will end here -- not everything that we have as secure information needs to be secure information --

Mr. Scott. I agree 100 percent.

Mr. Alvarez. -- right? That is one of the things.

So we created essentially an intelligence committee called the Security and Threat Assessment Committee. We take law-enforcement-sensitive information -- because I can't get anyone to sponsor my other House members to get their secure clearance. If I could do that, I could open their eyes and I could teach them more about what the threat is.

But we just need more information and we need more training and we need more sharing.

Mr. Scott. Okay.

I am short on time. I will --

Mr. Alvarez. Yes, sir.

Mr. Scott. -- tell you, the counterintelligence training for local law enforcement I do think is something that we should to work on. And we can do that collaboratively --

Mr. Alvarez. Yes, sir.

Mr. Scott. -- you know, Federal grants to State agencies, the Florida Department of Law Enforcement, Georgia Public Safety Training Center in Georgia.

I appreciate you all being here. I am concerned about the fusion center funding. I am

concerned about the staffing at the fusion centers as well. We have some where we don't even have I&A staff, and that is something that we need to fix as we go forward. But I appreciate you are here and your input.

Be careful on I-75 when you hit the Georgia line.

The Chairman. The gentleman yields.

And with my apologies, Mr. Quigley, I recognize you. You were keeping a pretty low profile down there in the front.

Mr. Quigley. That whole average height thing.

Thank you.

Director Sena, at the beginning, you talked about barriers and disconnected systems. Could you do a little deeper dive on exactly what you are talking about? What are the exact barriers to this being more effective?

Mr. Sena. Well, over the years, you know, systems have been developed at the Federal level, and I call them "silos of excellence," because, you know, they are not connected to each other, out of design, out of coordination, out of who they -- the audience that they believe should be in those areas.

So, just between DHS and the FBI, we have the Homeland Security Information Network at DHS, as well as the Homeland Security Data Network for classified information. On the FBI side, they have -- and I should also mention on the HSINT side, there is also the HSINT Adobe Connect for real-time information-sharing -- so, actually, more than one system there.

And then on the FBI side, you have the Law Enforcement Enterprise Portal Virtual Command Center; you have the eGuardian system, where the tips, leads, and, kind of, threats that come through that are being triaged go into.

But none of those systems connect to each other. And what you end up having are analysts that, even during major events, are having to simultaneously post things. And I use this example all

the time: During our Super Bowl, we had seven different systems that were live with different pieces of information in it. That means that, from a fusion center perspective, you have to have the same information go in sometimes seven different times into systems just so you can reach the audience that you are trying to reach.

The other barrier on that is that there is a differentiation on the FBI side, in their world, of who is allowed into their spaces, which is focused on law enforcement, but there is a whole community outside of law enforcement that needs to be part of this information-sharing environment.

And then when you start talking about the more classified material that oftentimes we are going to find within our counterintelligence realm, you are going to talk about Top Secret and SCI clearances that people would need to have to even access the data if they could get to it.

So, with all these systems and the lack of connectivity -- I have recently had some very good conversations with leadership at DHS I&A and FBI about how do we move towards a future vision of what collaboration looks like, so, that way, we are not pointing people into these silos, with an inability to actually find things sometimes.

Mr. Quigley. How do they connect? Who connects them? What is the platform between States and the Fed and between States? How would that work in the best of circumstances?

Mr. Sena. I mean, even at the unclassified level -- and I used this as an example during the World Cup, is that we at least came to some agreement to actually be able to use a platform that FIFA agreed with, their FIFA intel team, where we combined Microsoft Teams -- because everyone -- majority of States have it; there are a few Google States, but majority of folks had the Microsoft, you know, Office 365 suites. All of the Federal agencies have it. And we actually combined that with Esri geospatial technology and the one platform that we then could combine thousands and thousands of people across the country that could see events but at a baseline -- people could see what was happening at an unclass level, non-law-enforcement-sensitive

level -- and then downstream we had an ability for a smaller group of people, a couple thousand law enforcement officers across the country, to be able to share law-enforcement-sensitive information.

We need to look at formats and tools like that.

The other problem we have is identity management. I can't tell you -- it took me 6 hours to get DHS the ability to identify that I was actually a person that worked in the United States. I mean, true, my identity is a little obfuscated because of the work I used to do in law enforcement. But they ultimately had to sign me up as a foreign agent to be able to log in to the system. And I could tell you, it takes sometimes days for people to get into systems or weeks or months to be able to get in platforms.

And then their password changes every 90 days, so then they potentially get kicked out because they have to refresh their password. I am currently waiting for my password reset through the mail, because I need to reset my password.

Mr. Quigley. It's not your pet's name, is it?

Mr. Sena. No, no, no, not that.

Mr. Quigley. All right.

Well, look, a much longer answer, but I appreciate that. Thank you.

Mr. Sena. No worries. It is a complex mess.

Mr. Quigley. Got it.

Thank you.

The Chairman. The gentleman yields.

Mr. Hill?

Mr. Hill. Thank you, Chairman. And I really appreciate you convening this hearing. I think it is great to have these viewpoints from our States. Very keen.

And for the last 2-1/2 years, I have done quite a bit of work with the Arkansas Army and Arkansas Air National Guard. We have the 223rd Cyber Squadron in Little Rock -- Little Rock airport.

And Mr. Crawford and I share our representation for the State of Arkansas, along with Senate Chair Tom Cotton. So we are certainly attuned to this CI risk. And I just wouldn't disagree with a thing I have heard today from colleagues on both sides of the aisle.

But I want to narrow this to the topic that the chairman raised about the National Guard, because I have really been benchmarking this in other States.

Just this week, this 2-week section, Cyber Shield is underway right now at Camp Robinson in Little Rock. Eleven hundred people, 44 States, 23 countries. And everyone there is geared toward tactical action-taking against a cyber threat, state cyber actor. And I think that this training should be expanded.

And one of the things that I see is that we don't have any tabletop exercises on an operational attack to a civilian location. It could be Walmart. It doesn't have to be a water system. Everything we are practicing -- water system, water system, water system. We are just -- our brains are exploding with testing our water systems, when I think it is much more likely that the Chinese will, you know, destroy telecommunications in Bentonville, Arkansas. If you are going to disrupt Americans, no better way than to take down all of Walmart's stores.

So I think this integration is important. I agree with the SCIF comment. But I think tabletop exercising -- we do that for nuclear attack, we do it for all series of different kinds of civil defenses postures, but we don't do it in cyber to the extent I think we should.

So I think CI is important, but I think, because it's a law-enforcement exercise, it's a defense-of-the-homeland exercise, it has to be fused. But I think we need to really have an integrated approach.

So a couple of questions.

I heard people say they agreed with the SCIF exercise. But on the National Guard, back to Rick's point on that, North Carolina has a civilian workforce, paid by the State legislature, under the rubric of the National Guard doing cyber defense. So they are doing tabletop exercises routinely

with Duke Energy or Bank of America-Charlotte where they are doing precisely what I am talking about. And they have gone and put State resources at work in National Guard.

Do any of your States have that kind of either CI or cyber National Guard employees paid as civilians but under the Guard's rubric, mandate?

Mr. Alvarez. Sir, I am not aware of a civilian workforce under that, but Florida is kind of taking the lead in different ways.

We have established something called Cyber Florida. It is housed at the University of South Florida. And we have created essentially an electronic tabletop that is available to everyone and anyone in the State that is vetted. So, for example, if you want to pressure-test your company, you go to Cyber Florida. We create this electronic tabletop online, and we can test you, we can pressure-test you, we can attack you.

It's a little bit above my very simple brain when it comes to -- but they are very excited about it. And every single time you go speak to the business folks that have used it or the outsiders within the infrastructure that we have funded to do it, the results and the reactions are extremely positive.

We have also just funded $30 million to create a cyber center completely focused at the University of South Florida for this exact purpose of research --

Mr. Hill. I love it.

Mr. Alvarez. -- as well as individuals. Because we understand, like, the defense part is -- they are doing their thing, but we are vulnerable in all sorts of areas, and we have to train folks in that mindset, as well as in those skill sets, to get out in the field and defend us.

Mr. Hill. I think that is a great example.

And, you know, my point is that we call out the Guard or, in our case, the Air Guard, you know, to deal with New Madrid fault or a practiced civic defense on a nuclear launch or something like that, but what about calling out the top cyber warriors that are living in Little Rock, Arkansas, who are Air National Guardsmen, to go to Bentonville to the Walmart center and plug in? And you

can't do that without a plan.

And so, anyway, I think this is important. I commend the chairman for the hearing today. This has been very interesting. And we are grateful for your service.

I yield back.

The Chairman. The gentleman yields.

Dr. Jackson?

Dr. Jackson. Thank you, Mr. Chairman.

I thank the chairman, and thank you to our witnesses for being here today.

For many years, the Americans have believed that the counterintelligence threat from the Chinese Communist Party was focused solely on the Federal Government -- our intelligence agencies, our military, and our Federal research institutions. But the CCP does not confine its efforts to Washington. It has taken deliberate steps to infiltrate State and local governmental entities, universities, and critical infrastructure systems across the entire United States.

What makes these threats especially concerning is that we are asking our State and local officials to defend against these sophisticated state actors with a fraction of the tools and resources that the Federal Government uses to defend itself.

The U.S. and China are actively in a competitive race to achieve global dominance in artificial intelligence and computing. Winning this race is imperative for America's ability to maintain its economic and national-security dominance.

Mr. Sena, my home of State of Texas has recently seen a massive increase in AI data-center development and energy infrastructure projects, as I am sure all of you have in your home States as well. However, these huge economic investments have also seen a significant amount of scrutiny regarding water usage, rural development, and power-grid strain.

Have you seen instances of foreign malign influence, China in particular, affecting the public perception of data-center developments across the U.S.? And if you have, how is this happening at

the local level? Can you describe to us here exactly how this is taking place?

Because it seems like it is taking place on a very, very basic level. It is making its way into city government, city council discussions, things of that nature. It is completely changing the public perception of what is going on and turning the American people and these communities against data centers, which, as I just mentioned, we are going to have to find a way to develop and compete.

Mr. Sena. You know -- and I have to say that, at every level of State and local government, we are seeing foreign malign influence, these actors trying to -- even at the local city councils -- trying to do outreach, trying to coordinate, trying to contribute to campaigns in various ways. And so the problem is, if there is anything that would advance our country, their goal is to disrupt that.

And so that is what we are seeing, is that folks at the local level. I talked about that mayor earlier that, you know, ended up pleading guilty about, you know, 2 months ago, but she was basically working out there on a website, posting things specifically to maneuver the population, whoever is looking at that website, to that party's ideology, and very much at the detriment of U.S. citizens and the detriment of our country and the ways and the tools that we are trying to advance to be ahead of those countries.

That is their goal -- disrupt us. And they are being much more effective than we are at stopping that.

Mr. Alvarez. Sir, most anything anyone knows about an AI data center they have learned from TikTok.

Dr. Jackson. Right.

Mr. Alvarez. China is not going to beat us in the modern battlefield with a bullet and a gun; they are going to beat us with one post at a time.

And the reality of the matter is -- we go back to the very question I answered before from Mr. Scott -- it is about education. Most people don't know they are the receiver of a foreign operation against them to influence their mind. If I win your mind and you can come out against

that data center -- and I am not saying that some of those things aren't true. The reality is, what I am saying is, I don't know what to believe anymore, because I don't know if the data you are giving me is a Chinese operation to work against me because they are trying to build their AI data centers while they work against us or not. And that is the real problem here.

So we go back to what -- we have to get to the building block of education, telling people that we aren't simply best friends with China, that is not where all of our stuff comes from. They are an active worker against us. They are the enemy on many fronts. But most people don't even know that.

And so, when they see that TikTok, they are like, "Man, they are using a lot of water." Within 10 years, they won't even be using water because the scaling of those centers will be so small because the data processing is so fast and so big on a smaller scale. But the entire time, the Chinese are building and we are not.

Dr. Jackson. Yeah, I agree with you. And the education is a huge part of it --

Mr. Alvarez. Education.

Dr. Jackson. -- because even I didn't know that it was happening at the local level until I started hearing about it in large numbers and then started digging into a little bit about where is this coming from and then realizing that it was coming from Facebook and from TikTok.

But there are people out there that are being paid, that are, you know, on salary somewhere, that are being paid to start this and get this misinformation, you know, project up and moving. And I think that we have to be able to find these people, as well, and figure out what they are tied to and how they are tied to the PRC or some, you know, other malign actor and figure out a way to stop this as well.

Mr. Alvarez. Well, sir, I will give you another example. When I ran that CI bill about creating the CI team, it sailed through the first two committees almost unanimously. But somewhere along the way, someone sends me a post that "Danny Alvarez is trying to create the

Jewish secret police to come after your personal private information and your political thought."

I blew it off as a laugh, right? Because it was like, that is so crazy, why would anyone believe that? They then sent to me -- at the end of the session about a month later, it had over 9,000 shares -- not likes; shares. That means 9,000 people believed it enough to pass it along.

That is the kind of stuff we are talking about. They don't need to beat us on the battlefield if they beat us before we even get there.

Dr. Jackson. Yeah. I agree. Thank you. I guess we have some educational efforts I hadn't heard of that we need to address.

And my time has expired. I thank you.

The Chairman. Mr. Crenshaw?

Mr. Crenshaw. Thank you.

Thank you all for being here.

You know, counterintelligence has historically focused on, you know, traditional hostile actors, a spy in our midst. But it is very different now. And it is very hard to distinguish between what -- you know, if a Chinese businessman is doing activities like buying up land, leasing storage units, contracting with a trucking company, you know, from my perspective, I see what that is. That is preparation of the environment. But that is what the new counterintelligence threat is.

And, you know, how are you guys dealing with that? And is that kind of training, knowing what to look for, does that exist at fusion centers?

I guess this question might be for Mr. Sena.

Mr. Sena. And that has actually been -- over the years, you know, we have blended that counterintel threat, because the same things that we are looking for for a suspicious activity related to a counterterrorism threat -- you know, the elicitation, the surveillance -- all those things click a number of boxes that need further investigation, further followup.

But who would have thought a person in the middle of a cornfield repeatedly going out there

early in the morning would draw anyone's attention? Until someone actually went out there and talked to the person and found out that they were stealing the corn to send it back to China.

Mr. Crenshaw. Yeah.

Mr. Sena. I mean, those are the things that we miss if people don't look or know what to look for. How many times are those opportunities to intersect with a counterintelligence threat missed if that officer or that person out there in the field don't know the right questions to ask?

And we have had that happen. Cops have sat there and talked to four different people in a car with four different stories of what they were doing. And so those are the clues.

Mr. Crenshaw. And these actors are operating within legal limits. It is difficult.

So, related to that, you know, how is our information-sharing ecosystem?

Because a lot of this information is coming from, you know, local governments, online, university settings. And then, of course, there is the information-sharing with, say, the National Counterterrorism Center.

How is that going?

Mr. Sena. You know, on a scale, I see many lanes right now where we have fallen behind. I mean, I have been doing this since September 11th, as far as the fusion center business, and I have seen some of the things. I mean, we have had huge leaps and bounds in the first 10 years, first 15 years. But, you know, especially over the last 5, I have seen some of the things breaking, I have seen some of the things that we had previously that aren't there anymore.

Even on the counterintelligence side. You know, I used to go to the National Counterintelligence and Security Center and brief 300 people on the importance of what fusion centers do and how you should connect. They had videos that they made about how these foreign actors are coming into the country and taking advantage of us. But nobody is watching those videos. So --

Mr. Crenshaw. So, not good?

Mr. Alvarez. Not where we need to be. Not really.

Mr. Crenshaw. Okay. Yeah.

And I guess related to that, it doesn't sound like analysts that operate in these fusion centers are maybe receiving enough strategic context or classified information from Federal partners. Would you say that?

Mr. Alvarez. I think that was a good foundation of why our groups started out in September of 2023 to actually share information across fusion centers related to counterintelligence information.

Mr. Crenshaw. Well --

Mr. Alvarez. A number of reasons -- classification, lack of training. But our own personnel said, we need to do something --

Mr. Crenshaw. But bottom line is it needs it improve?

Mr. Alvarez. Absolutely, sir.

Mr. Crenshaw. Mr. Lucci, can you describe in more detail what you saw with the Chinese interference in Texas legislative efforts?

Mr. Lucci. Congressman, September 10, 2024, there was a hearing in Tyler. That hearing ended because of a cyber attack that -- I don't know the sourcing of the cyber attack, but the hearing was the Texas CCP committee on September 10, 2024. The cyber attack took over the live feed, it played a number of very unseemly things over the live feed, and then the committee actually just got shut down.

Mr. Crenshaw. Wow.

Mr. Lucci. I have heard that there was potentially a bomb threat.

Another date I would point out: April 2, 2025, when the legislature was in session, not in interim. There were 11 bills heard on 1 day in the Committee on Homeland Security, and those 11 bills were objected to by Chinese nationals across the board who spoke to these bills. They were

speaking to totally different issues.

Mr. Crenshaw. Hm.

Mr. Lucci. There was one individual who graduated from a Seven Sons of National Defense university who testified against eight of these bills, and he was reading off of the consulate web page as he did so. There were Chinese --

Mr. Crenshaw. I am going to cut you off. I wish I could hear all these stories, but I really want to get one more thing on the record here, which is -- and it was brought up before, about counter-drones.

It is apparent to me that local law enforcement nor private owners of critical infrastructure have the legal ability to deal with drones if they come into their airspace, correct? This is a huge problem.

Mr. Alvarez. That is correct.

Mr. Sena. Yes, that is correct, sir.

Mr. Crenshaw. Big problem.

Thank you. I yield back.

The Chairman. Mr. Fallon?

Mr. Fallon. Thank you, Mr. Chairman.

So, when the hearing began, I was listening very carefully to what the chairman said, what the ranking member said, what all the witnesses said. And I didn't disagree with literally anything that any of you said. I fully agreed with it.

And I got to thinking about where the -- the fusion centers began, you know, to kind of root out and protect us against terrorism, right? And then it became this counterintelligence threat because of the rise of primarily China and the fact that they have this incredibly large economy, second-largest in the world, and they have resources the Soviets never had. And that really gives me pause.

So, when I think about, if I were in Beijing, what would I do -- and I don't want to delineate the exact things because maybe I am giving them an idea. Probably not, but they are pretty slick at what they do. But I don't think it is science fiction to think that a country with this kind of nefarious intent and the resources would be planting sleeper agents in the country, particularly when we have had such a porous border over the last 4 years, and looking at how to attack infrastructure if we ever got into a hot war with them, God forbid, if they crossed the Straits -- transportation, energy, food and water supply, comms and other critical infrastructure -- and putting Americans that either powerful or creating Americans that are powerful to put them in those positions and use them as friends of China, whether they are useful idiots or they are knowingly collaborators, and using any and all means at their disposal for corporate and tech espionage, which I think they are doing in large measure on the West Coast particularly, and also exploiting birthright tourism, and, of course, influencing their elections as well.

They don't need to get into a hot war, nor is that their intent. We got briefings on that that were non-classified years ago. They would rather see the decay and malaise, if you will, to use a Jimmy Carter term from a very long time ago, the American malaise, and chip away at us, divide us, balkanize us, divide us on gender and class and race and religion.

And I am going to tell you, and I will share something with you, and it seems like -- it was an epiphany for me. The World Cup, you had the Mexican national team, they are playing in Mexico City, they played the Mexican national anthem, and every single one of those players had their hands on their hearts and they were singing that national anthem with pride. They were proud to be Mexican.

And if you don't have Americans that are proud to be American, like, with that kind of enthusiasm, you will lose this Republic, and not today, not tomorrow, but you eventually will.

And that is another reason why the Chinese communists are using their soft power in K through 12 but specifically in the universities.

So, Mr. Lucci, I want to talk to you a little bit about this birthright tourism exploitation that they really seem to be doing at scale -- coordinated abuse at scale in Saipan.

Did you testify in June in a committee hearing?

Mr. Lucci. Yes, sir.

Mr. Fallon. And that was the China Select Committee?

Mr. Lucci. Yes, it was.

Mr. Fallon. Were you accused of racism?

Mr. Lucci. I was, yeah.

Mr. Fallon. Yeah. I just saw the clip. I stepped out and I wanted to see the clip, and I thought it was absolutely ludicrous and don't really want to get into that per se.

But talk to me a little bit about the scale that we are talking about in Saipan -- and I think it is mostly the Northern Mariana Islands -- and what China is doing.

Mr. Lucci. So the first issue is, I believe they have visa-free travel there.

Mr. Fallon. Yeah, I think that is the case.

Mr. Lucci. And separate from birth tourism, that --

Mr. Fallon. And they can stay as long as they want, right? There is no restriction?

Mr. Lucci. Well --

Mr. Fallon. Or it is a long time.

Mr. Lucci. -- if they could go in there, then they could fly to the continental United States. So it is an open door to our entire backyard. And that is if we catch them.

You know, I have seen estimates, 750,000 to 1.5 million essentially born of Chinese couples but then brought back to China and --

Mr. Fallon. Up to 1.5 million.

Mr. Lucci. That was from a Senate Judiciary or House Judiciary Committee of March this year where they discussed those numbers of -- this isn't birthright; this is birth tourism, which has

very low support amongst the American people.

Mr. Fallon. Yeah, right, birthright and birth -- this is an abusive of, really, birthright tourism. You are talking about bringing someone that is pregnant and bringing them to the country, they have the child, then they immediately go back to home country, right? That is what we are talking about.

Mr. Lucci. Right. Right.

Mr. Fallon. Yeah. And then that person, that child is raised in that foreign state, which is an adversary nation to the United States.

Mr. Lucci. That is right.

Mr. Fallon. Would you have the same passion and feelings if they were Russian?

Mr. Lucci. We look at who you all define as Federal adversaries.

Mr. Fallon. Uh-huh.

Mr. Lucci. China, Russia, North Korea, Iran.

Mr. Fallon. So Russia is.

Mr. Lucci. Russia is, yes.

Mr. Fallon. Yes. And you would have that same apprehension if you had, say, 1.5 million Russians that were born in the United States and then immediately brought back to Russia, which is a foreign adversary?

Mr. Lucci. If a lot of Vladimir Putin's friends were coming over here and getting citizenship that way, I think it would be --

Mr. Fallon. They don't have the United States' best interest at heart, do they?

Mr. Lucci. -- it would be a significant concern, yes.

Mr. Fallon. Now, would I call you a racist if that were the case? "How dare you bring more White people over here and then get them back there." It makes no difference, right?

Mr. Lucci. That is right.

Mr. Fallon. I think that was disgusting, that you were accused of that, considering your

personal journey as well. And, again, we don't need to get into it. But it is unfortunate when some people are running for President what they will do.

But you are talking about protecting the United States homeland and all its citizens, including the millions that are ethnically Chinese, correct?

Mr. Lucci. Those are the main targets. And I think that that needs to be made clear. I mean, the Chinese leader has made clear that he wants to leverage the Chinese diaspora within the United States and other countries. And so the way that works is, they surround and abuse people who speak out against the regime and they reward people in the United States who favor the regime.

The New York Times covered this, 50-some organizations in the City of New York, to make sure anti-CCP candidates in New York cannot get elected -- in America --

Mr. Fallon. Uh-huh.

Mr. Lucci. -- cannot get elected.

Mr. Fallon. Yeah. They do it domestically. They are going to do it internationally as well. No surprise.

Mr. Lucci. This happens all over.

Mr. Fallon. Unfortunately, my time is up. Thank you very much.

Mr. Lucci. Thank you.

Mr. Fallon. And thank you to all of you for the great work you are doing.

Mr. Chairman, I yield back.

The Chairman. Mr. Krishnamoorthi?

Mr. Krishnamoorthi. Okay. Thank you, Mr. Chair.

Mr. Moseley, I recently learned of an incident in which the Alabama Fusion Center received a tip that it shared with the Chicago Fusion Center to help them discover and arrest a person with, quote, "a basement full of weapons and his own shooting range, where he was training to kill some folks in Chicago."

Mr. Moseley, it is fusion centers like yours that are able to help thwart and prevent these types of terror attacks like this potential one in Chicago, right?

Mr. Moseley. Yes, sir, that is correct.

Mr. Krishnamoorthi. And, Mr. Sena, the 80 or so fusion centers that you represent are State-owned and -operated, but they receive significant Federal funding from FEMA's Homeland Security Grant Program, correct?

Mr. Sena. That is correct, sir.

Mr. Krishnamoorthi. President Trump, however, has put that funding at risk. Last week, The New York Times reported that the administration is demanding that, quote, "States change voting rules or lose anti-terrorism funds," including this particular Homeland Security Grant Program funding.

That is what this headline says, correct?

Mr. Sena. That is correct.

Mr. Krishnamoorthi. So I went to grants.gov -- or my staff did, I should say -- to look at FEMA's notice of funding for this year's grant that should fund your fusion centers. And there is an entirely new section in that grants.gov that says the following: "Funding Withholding for Election Security NPA Requirements."

It states that, quote, "recipients must comply with [new election] requirements as a condition of full drawdown of [grants]" and FEMA will withhold 20 percent of the grant until States provide, quote, "proof of compliance."

That is what it says, right, sir?

Mr. Alvarez. That is correct.

Mr. Krishnamoorthi. These now requirements would force States to transition to paper ballots, verify citizenship of voters, and make other changes to election procedures in line with the President's entire election agenda.

Mr. Moseley, we shouldn't be attaching any additional strings to the vital anti-terrorism funds that your fusion center receives, right?

Mr. Moseley. Correct.

Mr. Krishnamoorthi. Any less funding for your fusion centers could impact our ability to prevent terrorist attacks, right?

Mr. Moseley. It is not going to affect our ability; we are going to continue the mission regardless of that. We are in it -- we are going to be in it. So, whether you cut that funding or not, we are still going to do our job.

Mr. Krishnamoorthi. But all things being equal, if you have less finding, you have less capabilities to do your job, right?

Mr. Moseley. If we have less funding, we will have less staff; there will be more on the staff that are there.

But we are going to continue to do our job and fight that fight, just like the one that you mentioned between us and Chicago --

Mr. Krishnamoorthi. You will have less resources.

Mr. Moseley. Yes, sir.

Mr. Krishnamoorthi. Yeah.

I believe we shouldn't be conditioning any anti-terrorism funding on any agenda related to the election-security issue, because I think that we have to fight terrorism with all resources possible.

Let me transition to my next topic.

President Trump announced that tomorrow he will hold a prime-time address regarding election security. Reuters and New York Times reported that Trump will discuss, quote, "voting machines and may declassify documents to raise concerns about potential foreign interference."

Mr. Sena, you have covered State-level counterintelligence capabilities throughout your career, including the 2020 election, right?

Mr. Sena. That is correct, sir.

Mr. Krishnamoorthi. In a 2021 National Intelligence Council report, the Intelligence Community reported that, quote, it "has no indications that any foreign actor attempted to interfere in the 2020 U.S. election by altering any technical aspect of the voting process."

That is what the IC concluded, correct?

Mr. Sena. That is correct.

Mr. Krishnamoorthi. And, sir, you don't have any evidence contradicting the NIC, or the National Intelligence Council, estimate, correct?

Mr. Sena. That is correct.

Mr. Krishnamoorthi. Because there is none.

If the President were really concerned with foreign countries attempting to interfere or influence our elections, he should be increasing Federal support for security, not scaling it back.

The Election Assistance Commission is one Federal agency, created by Congress more than 20 years ago, to help State and local officials conduct elections, including training them on the latest voting technology.

But, Mr. Sena, last week, Politico reported that Trump ousted the remaining members of the bipartisan Election Commission ahead of the midterms. You don't dispute that, right?

Mr. Sena. I saw that. Correct.

Mr. Krishnamoorthi. And take CISA, our Federal agency for cybersecurity infrastructure. The President actually created CISA in his first time term.

Isn't that right, Mr. Lucci?

Mr. Lucci. Congressman, I assume that is correct. I don't really track who created CISA, though.

Mr. Krishnamoorthi. Okay.

Mr. Lucci. I operate at the State level.

Mr. Krishnamoorthi. Okay.

According to both the --

The Chairman. The gentleman's time has expired.

Mr. Steube?

Mr. Steube. Mr. Moseley, does Alabama have voter ID? Identification required to vote?

Mr. Moseley. Yes, sir.

Mr. Steube. So, to Mr. Krishnamoorthi's point, you wouldn't lose any Federal funding. Is that correct?

Mr. Moseley. That is my understanding. Yes, sir.

Mr. Steube. Mr. Sena, California -- if the President's announcements today -- tomorrow -- Wednesday is -- Thursday -- if his announcement tomorrow is regarding the Georgia election fraud and the declassifying of documents -- you are from California, right?

Mr. Sena. I am, sir.

Mr. Steube. So you would have absolutely zero knowledge whatsoever of anything that occurred in Georgia. Is that correct?

Mr. Sena. That is correct.

Mr. Steube. Thank you for that.

All right. Moving on to Mr. Alvarez, first of all, thank you for being in Tampa for our event for HPSCI.

Mr. Alvarez. Yes, sir. Thank you.

Mr. Steube. Can you describe what your CI is supposed to look like and do?

Mr. Alvarez. Yes, sir.

So FDLE is divided over seven regions. We were going to put one team in each region. Thirteen members. To become one of those members, you had to have a CI background. Either you had to have some experience at the Federal or a State level having done that. And then those

13 members will be made up of actual agents in the field, analysts, and then -- as well as cyber analysts as well. That is going to operate in tandem with State and Federal resources.

And one thing that was very important, sir, to point out is, they were dedicated only to CI. They could not be cross-used for anything else. You know, they couldn't take them to go do a DUI or do some sort of any other work other than CI-related. The focus is to protect that area.

Mr. Steube. And is this the only CI-related idea that you are running or considering?

Mr. Alvarez. No, sir. We are actually going extremely granular. The list of bills that we are considering is going -- we are going as granular as unifying 911 centers so that we can have operational battlespace vision and communications ability.

We are proposing a CI directorate. We are talking about unifying State law enforcement in something similar to what Texas has into the Florida Department of Public Safety -- not creating a new State police, but just reorganizing so that the one director that is in charge of intelligence and counterterror can have control of his assets, or her assets.

Reporting requirements in education. Transnational oppression. Public-private partnerships trying to create actual infrastructures to teach the business owners. And we have got lists going on, sir.

So this is just step one of a -- it will continue after I am not elected anymore. That is the bottom line.

Mr. Steube. So the bill that you filed, you kind of discussed it in your opening comments; it is also in your written testimony. It didn't pass this year. I assume you are intending on filing that next --

Mr. Alvarez. Yes, sir.

Mr. Steube. -- legislative cycle?

What was the challenge? Was the House the challenge? Was the Senate the challenge? Was it people just not understanding what the issue was? Can you just walk me through the

politics of that?

Mr. Alvarez. No, sir, it was -- we ran out of time. So, at the end, when --

Mr. Steube. So did you make it through all your House committees?

Mr. Alvarez. We made it through three out of the four. So, on the fourth one, we ran out of time, and the session ended. That is what happened.

Ultimately, at the very end, when I told you the Israeli secret police -- when that information started coming out, there was a lot of discussion about individual rights. So what we are going to do this next time is, we are going to narrowly tailor it to make sure we identify exactly what it was, and we are going to re-file it coming this year.

Mr. Steube. So walk us through some of the specifics in that piece of legislation.

And then, to caveat onto that, or to add onto that, are there other States that have done or are doing similar things legislatively?

Mr. Alvarez. I am not aware of other States. In fact, when we first proposed this, sir, we started getting calls from some partners in the Federal Government, and we thought we were in trouble. Honestly, like, we thought we had stepped on toes. And, in fact, those people were encouraging us to do this. They hadn't seen it anywhere else. Or they had been encouraging people to do it, and we kind of just jumped on it.

Specifically, some of the things that -- what was your question again, sir? You were asking what happened?

Mr. Steube. Well, like, give me some specifics of what was in it.

Mr. Alvarez. Oh, okay. The layout of the team and what the mandate was. The mandate was pretty broad. And inside the mandate, that gave the critics the ability to say that we were going after individual civil liberties and rights and that we were trying to go after political thought. I understood where they were coming from, and we were beginning to edit the bill in its final stop before the session ended.

So it wasn't, sir, really one of those things where it was a lack of political will. It almost sailed unanimously each time. On the last one, it was a 25-member committee and it only got 5 negative votes. I predict it will go through the same way and in the Senate as well, sir.

Mr. Steube. And so -- I only have a little bit of time left, but -- the State of Florida requires voter identification. Is that correct?

Mr. Alvarez. Yes, sir.

Mr. Steube. So the State of Florida wouldn't risk losing any Federal funding as it relates to the President's executive order?

Mr. Alvarez. Not that I am aware of, sir.

Mr. Steube. All right.

I yield back.

The Chairman. The gentleman yields.

I want to thank the witnesses for being here today. It has been very enlightening. Appreciate your support.

Oh, Mr. Fitzpatrick, I am sorry. I didn't mean to -- you snuck in here. Mr. Fitzpatrick, you are recognized.

Mr. Fitzpatrick. Thank you, Mr. Chairman.

Senator Bostar, thank you for being here today.

The PRC is actively infiltrating State and local political offices and leveraging lobby groups and other proxies to conduct influence operations domestically here at home.

Can you describe some of the more aggressive or sophisticated tactics that you have witnessed to undermine lawmaking, specifically at the State level?

And, secondly, do you believe that adversaries like the CCP are scared to operate inside the United States or view the U.S. as a non-permissive environment?

Mr. Bostar. Well, I will start with your second question. And thank you for them.

No, I don't think that there is any reluctance from our adversaries to operate within the U.S., considering, in particular, that there is an extraordinary amount of evidence that they are, and constantly.

We have experienced -- through the last 4 to 5 years of us pursuing legislation and policy around putting in some protections against our foreign adversaries, we have experienced a wide variety of types of opposition, but I think that there are some things that are particularly important to call out as concepts, one of which is the nature of adversarial entities embedding themselves in larger associations, membership groups, that will then turn those groups against initiatives to protect Americans.

So, you know, for example, if we introduce a bill that requires foreign-agent registrations on a State level to try to, in particular, close a lot of the gaps that exist on fora on the Federal level, you know, we will end up with opposition from a technology association, right? And the reason being is that there is one entity who is a member that cares, and it is, you know, a Chinese company, let's say Alibaba, whereas no one else cares, right? The other companies that are involved don't care.

But the way it tends to work is, if someone cares, if someone wants to bring opposition to a policy, and no one else is particularly interested in that policy, then that whole organization stands in opposition.

And so we face an incredible amount of pressure, where groups that we will normally work with and that also are made up of entities that we work with every day are then read in and interpreted as being opposed to commonsense policies that we might try to pursue in order to just provide some more guardrails.

But the list of activities is long.

Mr. Fitzpatrick. Thank you, Senator.

Mr. Lucci, obviously, counterintelligence and securing our Nation must be a nonpartisan effort. It is evident through your work and the work of legislatures across our country that we are

seeing good bipartisan support for CI.

Can you highlight some of the most effective legislators that you have seen advancing bipartisanship and making proactive CI legislation which is making our States safer?

Mr. Lucci. Well, Congressman, number one is right down there. Senator Bostar, as a Democrat, works with the Republican Governor, passing the most effective legislation across the country.

You know, in the States of Texas and Florida, the most important legislation on higher education and many other bills had bipartisan sponsorship in both of those States. In many of the States -- you know, I remember the vote counts in Texas a lot better. But, like, in the Senate, 29-2. Lots of votes like that. Similar in the House.

And so, when there are clear objectives, clear leadership, and clear knowledge -- and that is what we keep coming back to today -- clear knowledge of the threat, there is a really good unity around these issues.

And I would just close with that. The more that you all can tell State leaders about what these gaps are and that they ought to take them on, they will just start going, and they will accomplish things that go beyond what you set them out on to begin with.

Mr. Fitzpatrick. Thank you, sir.

Mr. Chairman, I yield back.

The Chairman. The gentleman yields.

And, with that, I want to thank the witnesses once again for being here. Very enlightening. Look forward to working with you all in the future on this issue. Very important to our national security.

And, with that, this briefing is adjourned.

[Whereupon, at 3:48 p.m., the committee was adjourned.]