Written Statement for the Record

Mike Sena, President, National Fusion Center Association
Executive Director, Northern California Regional Intelligence Center (NCRIC)/HIDTA

Hearing: State-Level Counterintelligence Threats and Capabilities

House Permanent Select Committee on Intelligence
United States House of Representatives

July 15, 2026

Introduction

Chairman Crawford, Ranking Member Himes, and Members of the Committee, thank you for the opportunity to testify today on the counterintelligence threats that face our Nation at the state and local level. My name is Mike Sena, and I serve as President of the National Fusion Center Association (NFCA), representing the 80 state and major urban area fusion centers that make up the National Network of Fusion Centers.

I also serve as Executive Director of the Northern California Regional Intelligence Center (NCRIC) and the Northern California High Intensity Drug Trafficking Area (NC HIDTA), where our team works daily with federal, state, local, tribal, territorial, and private-sector partners on threat identification, intelligence analysis, investigative support, information sharing, and operational coordination in collaboration with the FBI's Counterintelligence Task Force, Joint Terrorism Task Force, DHS's Office of Intelligence & Analysis (I&A), Real-Time Crime Centers (RTCCs), Fusion Centers, High Intensity Drug Trafficking Areas (HIDTAs), the Regional Information Sharing Systems' (RISS) Watch Centers, and the Center for Internet Security (CIS).

I want to thank Members of this Committee for including the NFCA in the broader discussion on how our foreign adversaries have developed increasing capabilities against the homeland that

are not only impacting federal agencies and assets, but are also impacting the private sector, cities, counties, and states across our nation. Counterintelligence threats are compromising our nation's physical and cyber security every day, and we must leverage the National Network of Fusion Centers and their ability to connect and share information across all levels of government and the private sector.

Across the National Network of Fusion Centers, more than 3,200 personnel from state, local, federal, and private-sector partners collaborate to analyze threats, share intelligence, and support operational coordination, while safeguarding privacy, civil rights, and civil liberties. Since 2001, fusion centers have become a cornerstone of the homeland security enterprise, complementing federal partners such as the FBI's Counterintelligence Task Forces, Joint Terrorism Task Forces, the Homeland Security Task Forces, as well as other DOJ and DHS components. Fusion centers function as the primary hubs for consolidating threat information, coordinating across jurisdictions, and ensuring that actionable intelligence reaches decision makers and frontline agencies when it matters most.

There is no substitute for the National Network of Fusion Centers - they fill a unique role that cannot be replicated by any one entity. Working together with the Intelligence Commanders Groups of the Major Cities Chiefs Association (MCCA) and the Major County Sheriffs of America (MCSA), and in collaboration with statewide investigative agencies that are part of the Association of State Criminal Investigative Agencies (ASCIA), fusion centers play an essential role in helping to protect America.

Today, I will focus on how information sharing and counterintelligence collaboration should function, what we have seen work well, and where gaps remain - particularly in threat reporting, real-time coordination, staffing, funding, training, and access to counterintelligence information. I will also discuss the role of DHS I&A, the FBI, and other federal partners in supporting fusion centers, including the predictable, sustained resources and authorities needed to ensure this system functions effectively in the years ahead.

<u>The Changing Counterintelligence Landscape at the State Level</u>

Foreign intelligence services - most prominently the People's Republic of China (PRC), along with additional adversarial nation-state actors - are increasingly targeting state, local, and private-sector entities to obtain influence, access, and operational footholds. These threats have expanded well beyond traditional federal CI environments and now routinely intersect with local government, critical infrastructure, academic institutions, and private industry.

Our adversaries recognize that states oversee critical infrastructure, public research institutions, economic development, trade relationships, and sensitive policy engagements. As a result, state and local entities are often among the first to encounter emerging

counterintelligence indicators, especially where espionage, cyber activity, influence operations, and economic targeting overlap.

Counterintelligence is no longer solely a federal mission space; it is a shared national security responsibility requiring coordinated federal, state, and local action.

Across the country, State, Local, Tribal, and Territorial (SLTT) partners have encountered:

1. Subnational engagement attempts by foreign officials or proxies seeking direct access to governors, mayors, state agencies, and local leaders - sometimes without federal awareness.
2. Threats and intimidation of dissidents residing in the United States, including harassment, surveillance, and coercion by foreign security services or affiliated individuals.
3. Influence operations involving technology partnerships, cultural exchanges, or economic development initiatives conditioned on the use of foreign government-aligned technologies.
4. Business acquisitions and resource-area investments connected to parent companies in adversarial nations, raising concerns about supply-chain access and critical infrastructure security.
5. Unauthorized or unidentified unmanned aircraft system (UAS) activity over critical infrastructure, government facilities, and major public events

In my home state of California, the size, economy, global connectivity, innovation ecosystem, and concentration of advanced technology make it a high-priority target for foreign intelligence services. The state is home to world-class universities, research institutions, Silicon Valley, major ports of entry, critical infrastructure, and leading technology sectors. On average, California accounts for about 50% of all counterintelligence cases indicted by US DOJ annually.

Foreign adversaries, particularly China, Russia, and Iran, increasingly use blended tradecraft combining traditional espionage, economic and industrial collection, cyber operations, supply chain compromise, academic and research targeting, and foreign malign influence.

These threats are not abstract. They affect official travel, foreign delegations, research partnerships, public-private engagement, and access to sensitive information and technology.

On January 29, 2026, a former Google engineer was found guilty in San Francisco of seven counts of economic espionage and seven counts of theft of trade secrets for stealing thousands of pages of proprietary AI technology for the benefit of the People's Republic of China. The case marked the first-ever conviction involving AI-related economic espionage.

Between May 2022 and April 2023, the suspect secretly uploaded Google's confidential AI architecture, TPU and GPU system details, orchestration software, and Smart NIC designs to his

personal cloud account while simultaneously pursuing roles with PRC-backed technology ventures and founding his own PRC-based AI company. He claimed to investors he could replicate Google's AI supercomputing capabilities using stolen technology and applied to a PRC government "talent plan" to advance China's computing power.

Two months ago, a former mayor in California admitted in a federal plea agreement that she secretly acted under the direction of officials from the People's Republic of China. She helped operate a U.S.-based website that published PRC-directed propaganda and covertly posted content supplied by PRC officials, often responding to PRC instructions and reporting back on the reach of the posts. She also communicated with high-level PRC operatives, including a senior intelligence figure, to disseminate materials requested by PRC authorities. She also admitted that she failed to notify the Attorney General, as required by law, and did not disclose that the website hosted material directed by PRC government officials.

These activities underscore a central reality that foreign intelligence organizations now operate aggressively at the State and local level, exploiting gaps where federal visibility is limited and where existing systems were not built for counterintelligence detection.

Why States Are Building Their Own Counterintelligence Capabilities

For many years, counterintelligence (CI) has been seen as a federal mission space. But as threats have expanded geographically and operationally, and SLTT agencies are filling the vacuum left by significant gaps in the national CI posture.

Several factors explain the surge in state-level CI activity:

1. Insufficient Information Sharing Mechanisms

   Suspicious Activity Reporting (SAR) systems and national information-sharing standards do not fully accommodate CI-related indicators. SLTT agencies often receive information they cannot easily share with federal, state, local, tribal, and territorial (FSLTT) partners due to incompatible systems, unclear guidance, and issues related to the national security classification of the information.

   Existing federal platforms often cannot support real-time, multi-jurisdictional coordination, especially in fast-moving CI threat situations. DHS's Homeland Security Information Network (HSIN) and Homeland Secure Data Network (HSDN), and the FBI's Law Enforcement Enterprise Portal's Virtual Command Center (LEEP VCC) and eGuardian Portal do not have any connectivity to each other or the capacity to share actionable counterintelligence information.

As the Federal system of record for information sharing, this creates an alarming gap with state and local partners frequently operating with partial or delayed access to CI investigation details, even when personnel are properly cleared.

The Office of the Director of National Intelligence (ODNI) also previously had management responsibilities for the Program Manager for the Information Sharing Environment (PM-ISE), a robust Federal, State, Local, Tribal, and Territorial (FSLTT) Partnerships Group (FPG), and a State and Local Law Enforcement Partners' Federal Advisory Committee that together, helped support guidance on information sharing and promising practices to address threats to our nation.

The PM-ISE position led the efforts to connect the nation's FSLTT community with guidance developed to improve collaboration through Joint Regional Integration and Coordination Plans, SAR collection, and the protection of privacy, civil rights, and civil liberties. The PM-ISE's position was transferred to the White House and has not been filled for years. The ODNI's FSLTT partner engagement team's ranks have been reduced to the point of being unable to engage FSLTT partners. The State and Local Law Enforcement Partner's Federal Advisory Committee charter has not been renewed, and the committee members have not met in years.

Reestablishing a robust PM-ISE with authority to collaborate with state and local partners to improve intelligence information sharing policies and processes would be a helpful development.

2. Fragmentation of Federal Counterintelligence Operations

Counterintelligence tips and leads are often passed through multiple disconnected government channels, with no single workflow reliably consolidating them. This fragmentation means that SLTT agencies may be aware of emerging CI threats before federal agencies share corroborating details - forcing states to build their own analytic and coordination frameworks.

3. Expanding Reliance on State, Local, and Private-Sector Partners

Foreign adversaries increasingly target state and local officials, university research teams, small technology firms, and critical infrastructure operators. This moves the threat directly into domains where fusion centers already play lead roles at the state and local level.

4. Growth of Hybrid Threats

CI threats increasingly blend cyber intrusions, influence operations, coercion of diaspora communities, supply-chain manipulation, and criminal networks. SLTT entities deal with these hybrid threats daily and must develop CI competencies to respond effectively.

Emerging State-Level CI Capabilities

Many states, local governments, and organizations across the country are rapidly adapting, creating new CI-focused programs, structures, and expertise. Examples include:

1. NFCA Counterintelligence Subcommittees and State-Level Coordination

This year, the NFCA Counterintelligence Subcommittee was created with over 110 members from 23 states to coordinate CI threat discussions, reporting, and projects across the National Network of Fusion Centers. This includes regular meetings, joint production opportunities, and shared analysis on topics like foreign malign influence, transnational repression, and supply-chain risks.

2. Enhanced CI Threat Detection and Reporting

Fusion centers are increasingly integrating CI indicators into personnel vetting, technology procurement, critical infrastructure protection, and delegation travel assessments, and training for SLTT partners.

3. Local-Federal Embedded Partnerships

When federal partners embed personnel with fusion center personnel - as seen during major events like the Asia-Pacific Economic Cooperation (APEC) meetings in San Francisco, the Super Bowl and the FIFA World Cup Games in Santa Clara, California - information flow improves immediately. Real-time coordination dramatically increases local agencies' ability to detect CI threats. Inclusion of fusion center personnel as members of the FBI's Counterintelligence (CI) Task Force also provides training, clearances, and access to systems that improve threat detection, training, information sharing, and threat mitigation.

4. Cyber-CI Integration

Adversaries are leveraging cyber tools to target state and local systems, remote workers, and critical infrastructure. States are building cyber fusion capabilities to identify actors using AI-enabled identity obfuscation, fraudulent employment, and data-exfiltration methods.

North Korean IT workers are increasingly infiltrating U.S. businesses by disguising their identities and using U.S.-based individuals—both knowingly and unknowingly—to obtain fraudulent employment.

These schemes allow North Korea to bypass U.S. and U.N. sanctions and generate significant revenue for the regime. U.S.-based facilitators help North Korean workers obtain and use company laptops, establish remote access to U.S. networks, create job-search accounts, set up financial accounts, reship devices overseas, attend virtual interviews on their behalf, and even create front businesses that appear to offer contract IT services. Companies that outsource IT work face heightened vulnerabilities because they are further removed from the hiring process. These activities pose serious security risks to U.S. businesses, as well as state and local government agencies.

While our adversaries are gaining capabilities and access to our IT systems, our methods of identifying cyber threats are falling behind because of our inability to develop actionable information in a timely manner. Our partners at the FBI currently lack the administrative subpoena authority to access emerging cyber threats and share that threat information with fusion center personnel. This gravely limits our ability to identify cyber threats and cyber enabled criminal activity that impacts states, local agencies, critical infrastructure, businesses, and individual victims across the nation.

5. Counter-UAS (C-UAS) Detection as a Counterintelligence Capability Gap

Unauthorized drone activity over critical infrastructure, government facilities, and major public events is increasingly a counterintelligence problem, not simply a public safety one: a low-cost unmanned aircraft can conduct the kind of surveillance and reconnaissance that would otherwise require a human asset on the ground. Fusion centers are being asked to assess this activity, but additional resources are needed to detect or mitigate drone threats.

The Critical Role of DHS Office of Intelligence and Analysis

Within the broader information-sharing framework, DHS I&A plays a unique and irreplaceable counterintelligence role: it is the only element of the U.S. intelligence community statutorily charged with facilitating intelligence sharing with SLTT partners, including the National Network of Fusion Centers, on terrorism and other threats to the homeland — a category that increasingly includes the foreign counterintelligence threats detailed throughout this testimony.

From our perspective in the field, I&A is most effective when it is forward-deployed with access to federal information and the authority to appropriately share it with state and local partners. I&A personnel embedded in fusion centers enable a timely two-way flow of information and collaborative analysis, increasing the likelihood that threat reporting reaches state and local partners quickly while insights developed at the local level inform the national intelligence picture. During major events, this field presence can determine whether threat-related

intelligence arrives in time to help personnel on the ground recognize and prevent an incident - or arrives too late to be useful.

The Committee's inclusion of NFCA and our law enforcement partners in discussions on proposed legislative reforms to strengthen I&A's ability to support state and local law enforcement is welcome, and stakeholder input on those reforms is essential: decisions about staffing, authorities, release processes, and coordination mechanisms directly determine whether intelligence sharing works under the compressed timelines and heightened risk. Any reform effort should strengthen - not weaken - I&A's field presence.

Counterintelligence and Transnational Organized Crime Connections

In addition to the counterintelligence issues identified through fusion center reporting, recent investigative and intelligence support provided by the High Intensity Drug Trafficking Area (HIDTA) Program have highlighted several emerging trends that, while not traditional CI cases, reflect intelligence gaps and threat vectors that increasingly intersect with counterintelligence concerns as transnational criminal activities, foreign influence channels, and hybrid threat networks create CI-relevant vulnerabilities at the state and regional level.

HIDTA Investigative Support Centers have identified patterns of foreign actors engaged in criminal operations that frequently exhibit CI-relevant indicators—such as targeted engagement with local officials or efforts to gain footholds in critical infrastructure-adjacent sectors.

Recent HIDTA threat trend reporting indicates that certain drug-trafficking organizations operate with increasingly sophisticated transnational intelligence capabilities. These groups leverage foreign intermediaries, encrypted communications, spoofed identities, and complex financial concealment tactics. Their operational tradecraft—including counter-surveillance, insider recruitment, and exploitation of regulatory seams—creates overlap with CI threat patterns traditionally tracked at the federal level.

HIDTAs have also identified vulnerabilities within regional criminal organizations that foreign adversaries could exploit—intentionally or opportunistically—for access, influence, or intelligence collection. These include infiltration pathways through illicit finance, supply-chain dependencies, technology procurement, or personal networks with ties overseas. While these issues do not constitute fully developed CI cases, they illustrate how criminal ecosystems can become vectors for nation-state exploitation.

Collectively, these observations demonstrate that the CI threat landscape does not exist in isolation. Criminal networks, foreign influence operations, and transnational illicit markets increasingly blend together, creating hybrid environments where state-level partners - including

fusion centers and HIDTAs - must evaluate CI indicators alongside traditional criminal intelligence.

Resource Gaps Hindering State CI Response

Despite progress, several resource challenges limit the ability of SLTT agencies to scale CI capabilities:

Unpredictable federal grant guidance impedes staffing, analytical tools, and training needed to address CI threats. Fusion centers in many areas across the nation have not received their 2025 grant year funds in July of 2026, and some fusion centers have lost funding that will immediately reduce their operational capabilities to address major threats, including counterintelligence threats.

Limited access to federal systems and real-time information reduces situational awareness during major events and daily operations. Fusion centers across the nation have uneven access to the FBI's and DHS's classified systems, including top secret systems that are required to understand the counterintelligence threat landscape.

Security clearance delays prevent qualified fusion center personnel from participating in CI investigations and secure discussions. DHS provides Secret clearances to fusion personnel and on a case by case basis, Top Secret clearances. Clearance delays have existed due to the lack of personnel dedicated to processing state and local clearances. These delays persist because too few federal personnel are dedicated to processing state and local clearance requests.

Addressing these gaps is essential to a functioning, nationwide CI posture.

Recommendations for Strengthening State–Federal CI Coordination

To ensure our CI architecture reflects today's threat environment, I respectfully recommend:

1. Establish a National CI Information-Sharing Framework

   Prioritize resources to fulfill the duties of the Program Manager for the Information Sharing Environment (PM-ISE) and incorporate fusion centers as a component of the National Counterintelligence Strategy.

   Update the SAR functional standards to accommodate CI indicators and ensure interoperability across federal, SLTT, and private-sector partners.

   Continuing support and resources for the DHS I&A's field presence at fusion centers and ensuring that it is backed by a robust headquarters enterprise with access to relevant information from other federal partners and the Intelligence Community, as well as the authority to share appropriately with state and local partners including fusion centers.

Supporting the resources and authorities required to develop a joint single sign on DHS and FBI platform to securely share suspicious activity reporting (SAR) and counterintelligence information with fusion center personnel and their state, local, tribal, and territorial partners.

2. Expand Embedded Federal CI Personnel at Fusion Centers and Fusion Center Personnel Assigned to Counterintelligence Task Forces

Increase DHS I&A, FBI CI Task Force, and other federal agencies' presence at fusion centers to provide two-way intelligence flow that meets state-level needs. Provide fusion centers with the resources and clearances needed to participate in the FBI's Counterintelligence Task Force.

3. Invest Predictably in State CI Capabilities

Provide stable, timely grant guidance and flexible funding to support evolving CI mission sets.

4. Clearance Processes for State and local Fusion Center Personnel

Utilize reciprocity, provisional access, and expedited clearances to ensure that fusion center personnel can immediately contribute to joint CI operations.

5. Enhance Cyber-CI Integration Across Jurisdictions

Improve access to cyber threat indicators and build collaborative analytic environments across state and federal partners that also includes the appropriate administrative subpoena investigative authorities to access cyber threat information in a timely manner.

6. Training

Enhance resources and prioritization of SLTT training opportunities from the Director of National Intelligence's National Counterintelligence and Security Center.

Closing

Foreign intelligence services have shifted their focus toward state and local environments where federal visibility is limited, and adversaries can exploit jurisdictional seams. Many states are rising to meet this challenge - developing CI capabilities, building partnerships, and protecting communities. But the national counterintelligence posture must modernize to support them.

Fusion centers can play a key role at the center of this work, providing a unique space to connect local operational context with federal intelligence. When information sharing is timely,

coordinated, and properly resourced, CI threats can be detected and disrupted before they impact the public or vital national interests.

Thank you for your attention to this critical issue and for your continued partnership. I welcome your questions and look forward to working together to strengthen our nation's counterintelligence posture.