

PROTECTING U.S. GOVERNMENT AND BUSINESS LEADERS FROM CHINESE GOVERNMENT INFLUENCE OPERATIONS

OVERVIEW

For decades, a broad range of entities in China have forged ties with U.S. state and local government and business leaders. Many of these relationships often yield legitimate commercial, cultural, and educational benefits for both sides. However, as U.S.-China tensions have increased, the Chinese government—guided by the Chinese Communist Party (CCP) and specific branches within it, such as the United Front Work Department (UFWD)—has increasingly exploited these relationships to influence U.S. policies and advance China's strategic interests.

When partnering with any foreign entity, U.S. state and local government and business leaders should exercise caution, conduct thorough vetting, and build transparency and accountability into partnership agreements to guard against the risk of foreign government exploitation.

This document provides insights and practical steps to help U.S. leaders engage effectively while reducing risks from China's influence operations.

THREAT

China's approach to subnational engagement blends open diplomacy with covert and coercive tactics. U.S. leaders at the state, local, tribal, and territorial levels may unknowingly advance CCP agendas due to sophisticated and deceptive influence operations. Business opportunities or cultural exchanges that appear mutually beneficial may disguise China's underlying political motives. China also uses front companies and proxies, including non-governmental organizations (NGOs), to hide the true nature of these engagements and to maintain the covert, deniable status of its influence operations. The advancement of technology and social media has expanded the reach of these operations, making them even more challenging to detect. Furthermore, China may pressure U.S. companies to lobby officials at all levels to support China-aligned policies or oppose measures the CCP views as threatening.

The CCP's UFWD leads these influence efforts, coordinating with other Chinese government agencies and executing operations worldwide through various front organizations. Key Chinese influence actors include:

- The Chinese People's Association for Friendship with Foreign Countries (CPAFFC)
- The National Association for China's Peaceful Unification (NACPU).

METHODS OF INFLUENCE

INFORMATION COLLECTION

To identify targets for influence, China systematically collects and analyzes data—including personally identifiable information (PII)—from U.S. state and local leaders, business executives, and those close to them. Beijing employs social media, commercial databases, technical tools, and artificial intelligence—such as Chinese-owned DeepSeek—to build detailed profiles on individuals of interest, gain insight into their views, and identify vulnerabilities. China uses this information to conduct influence operations or for future leverage.

CYBER POSITIONING & TARGETING

China conducts a variety of cyber operations that set the conditions to target public and private sector IT networks, positioning itself within U.S. critical infrastructure systems for potential future exploitation. These operations range from broad network compromises to targeted intrusions against perceived critics and political figures.

> ***Case Example:*** In March 2024, seven hackers associated with the Chinese government were charged with a conspiracy spanning 14 years that involved computer intrusions targeting U.S. and foreign critics of China, businesses, and political figures. The hackers sent over 10,000 malicious emails designed to compromise email accounts, personal devices, and networks. They targeted federal officials, pro-democracy activists, and defense contractors across multiple countries.

MEDIA MANIPULATION

China uses state media and China-linked community organizations to shape narratives in its favor, influence local discourse, and pressure or intimidate critics in the United States. These efforts often include coordinated online influence campaigns that leverage social media, including fake or inauthentic accounts, amplification of preferred narratives, manipulation of online conversations on sensitive topics (e.g., China's human rights record, U.S.-Taiwan relations, and U.S. politics), and paid content placement. These operations also include transnational repression tactics that use intimidation and coercion to silence dissent among diaspora communities, Chinese nationals, and others in the United States who speak out against the CCP. Through these actions, China aims to extend its authoritarian reach beyond its borders, creating a chilling effect on free speech and democratic participation within U.S. communities, and to shape the information environment that informs public and policymaker decision-making at the federal, state, and local levels.

> ***Case Example:*** In January 2020, after the Taipei Economic and Cultural Office sent a letter to the Chicago Tribune, highlighting Taiwan's representation at the World Health Organization, the Chinese Consul General in Chicago responded by criticizing Taiwan's position and authority publicly. The Chinese Consulate General in Chicago also posted propaganda on its website attacking U.S. policies, disputing human rights concerns, and opposing Taiwan's independence."

PEOPLE-TO-PEOPLE DIPLOMACY

China (often through the work of UFWD and CPAFFC) uses "people-to-people diplomacy" to promote political objectives through non-state channels and subnational relationships (e.g., cultural exchanges, economic partnerships, and sister city agreements). While these business, technical, cultural, and educational exchanges may appear friendly and beneficial, they can be strategically exploited to advance CCP interests.

TARGETING FUTURE INFLUENCERS

China cultivates relationships with U.S. partners early in their careers, intending to leverage these connections as they rise to positions of influence. Investigations have shown how individuals positioned within state and local government can effectively advocate for pro-China policies once they gain significant authority.

> ***Case Example:*** In September 2024, an employee for a senior New York government official was indicted for violating and conspiring to violate the Foreign Agents Registration Act. The employee allegedly used her position to advance China's interests, including blocking Taiwanese government representatives from accessing high-level New York State officials and altering senior officials' messaging on China and the CCP.

POLICY & ECONOMIC INFLUENCE

China or its proxies may create economic dependencies among local business and government leaders through financial incentives, investment, and market-access pressures. Economic ties are often framed as being mutually beneficial, but they can lead to situations where U.S. officials and business leaders feel compelled to lobby for China-friendly policies and economic interests, or oppose measures China dislikes.

> ***Case Example:*** On 28 April 2024, the American Fujian Houyu Association celebrated its 40th Anniversary in Flushing, Queens, New York, bringing together 53 organizations with ties to China. Some of these groups have been known to promote China's interests, have connections with CCP officials, or have had significant interactions with the Chinese Consulate. According to Chinese news outlets covering the event, these attending organizations reportedly endorsed and fundraised for various New York political candidates.

ACADEMIC & RESEARCH EXPLOITATION

China and other foreign entities exploit research partnerships, Confucius Institute-style programs, student and scholar exchanges, and university donor relationships. While these can offer scientific and educational benefits, they pose a significant risk to intellectual property and national security when proper protections and transparency are lacking.

MITIGATION

U.S. officials and business leaders can preserve the benefits of engaging with China and other foreign entities while guarding against exploitation by building transparency, reciprocity, and accountability into these interactions. Key strategies include:

Stay Alert: Recognize that foreign partnerships often come with strings attached. Engage with clear objectives that align with U.S. national interests. Adopt or strengthen ethics rules requiring public reporting of foreign-sponsored travel and gifts, and prohibit undisclosed commitments.

Vet Partners Thoroughly: Conduct background checks on partners and prospective investors before establishing relationships or approving incentives or sales. Use resources like the U.S. Department of Commerce's Consolidated Screening List and the Department of Justice's Foreign Agents Registration Act (FARA) database to identify potential risks. Consider requiring ownership disclosure for land purchases and infrastructure deals. Before hosting trips or high-level visits, request and publish full delegation lists, funders, sponsors, and meeting agendas. Verify the legal status and beneficial ownership of companies or foundations offering investment or research support.

Ensure Transparent Agreements: Maintain transparency in all agreements with foreign entities. Require contracts and partnership documents to be publicly accessible. Contracts should state mutually agreeable, reciprocal objectives, and include clear termination and governing law clauses. Require legal review for intellectual property, data sharing, publication rights, and export control implications. Do not accept clauses that restrict future lawful contracts or speech.

Safeguard Academic Partnerships: For university or research and development agreements, vet contracts for intellectual property protection, publication rights, controlled-technology access, and compliance with export controls. Use institutional compliance offices and federal guidance when dealing with sensitive research. Be alert to transnational repression tactics impacting diaspora communities and students, and support policies that protect free expression while addressing credible threats.

Provide Education and Awareness: Facilitate workshops and briefings to educate local officials about Chinese government influence operations. Awareness is essential for informed decision-making.

Engage with U.S. Authorities: Maintain strong communication channels with federal agencies, including local FBI offices, the Department of Homeland Security's Office of Intelligence & Analysis state representatives, state fusion centers, and the Cybersecurity and Infrastructure Security Agency (CISA). Report suspicious activities and seek guidance to ensure alignment with national security protocols.

Uphold Democratic Values: When engaging with Chinese government representatives, affirm U.S. commitment to democratic principles and human rights. Ensure that discussions address not just economic cooperation but also the values that underpin U.S. policy.

Understanding China's influence operations at the subnational level is critical for U.S. leaders. By exercising caution and implementing proactive strategies, officials can reduce risks while preserving their decision-making independence and maintaining alignment with national priorities.

REPORTING

- **Covert influence, criminal outreach, or insider threats:** Contact your local FBI field office at www.fbi.gov/contact-us/field-offices.
- **Cyber incidents or network compromise:** Contact CISA (www.myservices.cisa.gov/irf) and your state chief information security officer or fusion center immediately.
- **Vetting partners and funding sources:** Use the Department of Commerce Consolidated Screening List and consult Department of Justice FARA disclosures.
- **Threat Information and Briefings:** State and local government offices may request regional threat information and unclassified briefings through their state fusion center or the DHS Office of Intelligence & Analysis.

For more threat awareness materials or publications, visit the National Counterintelligence and Security Center (NCSC) website at www.ncsc.gov or contact NCSC_Outreach@odni.gov.

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

INCIDENT REPORTING MECHANISMS

DEPARTMENT OF WAR

U.S. Army Counterintelligence Command (ACIC)

Submit an iSalute Suspicious Activity
call 1-800-CALLSPY (1-800-225-5779)
Report at https://www.usainscom.army.mil/iSALUTE/

US Army Criminal Investigative Division (CID)

Report tips online at www.cid.army.mil/Submit-a-Tip/

U.S. Department of the Navy (DON) 2X

Report suspicious incidents at https://report.eagleeyes.navy

Naval Criminal Investigative Services (NCIS)

Report at www.ncis.navy.mil/Resources/NCIS-Tips/ or call the NCIS Hotline (1-877-579-3648) or the NCIS Espionage Hotline (1-800-543-6289)

U.S. Air Force Office of Special Investigations (AFOSI)

Report at www.osi.af.mil/Submit-a-tip/

DEPARTMENT OF HOMELAND SECURITY

DHS Office of Intelligence and Analysis Private Sector Partnership Program

Call: 202-447-3517 or 202-282-9881
Report at oi&aprivatesectorcoordinator@hq.dhs.gov

Homeland Security Investigations (HSI)

Report at www.ice.gov/webform/ice-tip-form

Unites States Secret Service (USSS)

For suspicious activity involving surveillance of protected sites, unusual weapon acquisition, or threats against offices, contact your field security office:
www.secretservice.gov/contact/field-offices

Cybersecurity and Infrastructure Security Agency (CISA)

Report significant cyber incidents to the CISA Incident Reporting System (IRF) at www.myservices.cisa.gov/irf

OTHER FEDERAL AGENCIES

Diplomatic Security Service (DSS)

For national security threats, message
202-702-7843 via Signal, Telegram, or WhatsApp

National Counterintelligence and Security Center (NCSC)

For additional counterintelligence resources and awareness materials or publications from NCSC, visit our website: www.ncsc.gov

Federal Bureau of Investigation (FBI)

Report tips online at tips.fbi.gov or via phone at 1-800-CALL-FBI (1-800-225-5324). Contact your local FBI field office at www.fbi.gov/contact-us/field-offices