NATIONAL COUNTERINTELLIGENCE STRATEGY

2024

THE WHITE HOUSE

WASHINGTON

August 1, 2024

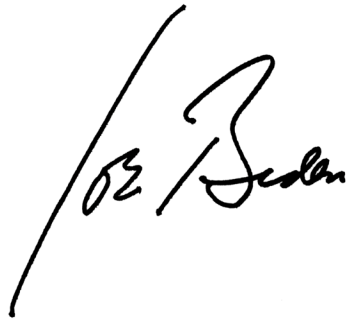
As President, my greatest obligation is to lead our Government in protecting the United States of America. A key part of that solemn duty is identifying and countering foreign intelligence threats directed against the United States and its allies and partners.

Foreign intelligence and security services and their proxies persist in seeking to acquire our most sensitive information, technology, and intellectual property. Non-state actors are following suit.

Foreign intelligence entities are also seeking to take advantage of the proliferation of commercially available tools to conduct surveillance; collect vast amounts of previously unavailable personal data; and position themselves to disrupt our infrastructure, industries, and institutions.

To keep pace with these threats, the National Counterintelligence Strategy provides strategic direction for the United States Federal Government and its counterintelligence community. Based on current and anticipated foreign intelligence threats, this strategy updates our counterintelligence priorities and aligns them with broader strategic priorities set forth in the National Security Strategy.

Above all, the National Counterintelligence Strategy supplies a vision that guides our efforts to work together to keep this country safe and ensures we are well-positioned to counter foreign intelligence threats.




NCSC
UNITED STATES OF AMERIC

Office of the Director of National Intelligence
National Counterintelligence and Security Center
Washington, DC

Our nation is facing significant and complex threats from aggressive and capable foreign intelligence adversaries—including Russia, the People's Republic of China, Iran, and North Korea, as well as other foreign state and non-state actors that are actively seeking to cause grave harm to the United States, its people, and institutions. The U.S. counterintelligence community is charged with identifying, understanding, and neutralizing foreign intelligence activities and capabilities in the United States; mitigating insider threats; protecting U.S. sensitive and classified information and sensitive facilities from technical penetrations, espionage, and other intelligence threats; and protecting U.S. interests, assets, and people at home and abroad from sabotage, assassination, or other foreign intelligence activities or operations.

This *National Counterintelligence Strategy*—developed by the National Counterintelligence and Security Center, in cooperation with partners across the U.S. Government and Intelligence Community—lays the foundation for a strategic counterintelligence program to prioritize and integrate counterintelligence activities to disrupt or compromise the ability of foreign intelligence entities to harm the national security interests of the United States, either domestically or abroad. It is designed to drive integration, action, and resources across the counterintelligence community to outmaneuver and constrain foreign intelligence entities, protect America's strategic advantages, and invest in the future to develop the capabilities and resilience needed to meet the current threats and challenges and those to come.

The scope, complexity, and urgency of the foreign intelligence threats facing the United States necessitates that we engage partners and audiences across the whole of society to share information, identify and mitigate vulnerabilities, strengthen our defenses and build resilience, and work together to combat these threats and overcome challenges to protect our people, institutions, and strategic advantages. The National Counterintelligence and Security Center is committed to coordinating this effort and to working with federal, state, and local governments, the private sector, academia, and our foreign partners to counter these foreign intelligence threats to our national and economic security and to our American way of life. ■


E PLURIBUS
UNUM

Vision

A Nation made more secure by a resilient and innovative counterintelligence community that protects the United States and its interests from foreign intelligence threats.

Mission

Identify, understand, and neutralize foreign intelligence threats and protect U.S. interests, assets, and people at home and abroad from espionage, sabotage, assassination, or other foreign intelligence activities or operations.

This *National Counterintelligence Strategy* provides strategic direction for the U.S. Federal Government and counterintelligence (CI) community for the next three years. It aligns CI efforts to national security priorities outlined in the *U.S. National Security Strategy* as well as other national strategies, and updates the CI communities' priorities based on the current and anticipated future foreign intelligence threat landscape. This strategy communicates these priorities to CI practitioners and our allies, partners, customers, and the public and provides a framework for strategic and operational planning, programming, resourcing, and evaluation. ■

Pillar One – Outmaneuver and Constrain Foreign Intelligence Entities
1. Detect, Understand, & Anticipate Foreign Intelligence Threats
2. Counter, Degrade, & Deter Foreign Intelligence Activities & Capabilities
3. Combat Foreign Intelligence Cyber Activities
Pillar Two – Protect America's Strategic Advantages
4. Protect Individuals Against Foreign Intelligence Targeting & Collection
5. Protect Democracy from Foreign Malign Influence
6. Protect Critical Technology & U.S. Economic Security
7. Protect the Nation's Critical Infrastructure
8. Reduce Risks to Key U.S. Supply Chains
Pillar Three – Invest in the Future
9. Build Counterintelligence Capabilities, Partnerships, & Resilience

The Foreign Intelligence Threat Landscape

The United States is facing threats from foreign intelligence entities[1] (FIEs) that are unprecedented in their breadth, volume, sophistication, and impact. An expanding array of actors are attempting to steal national secrets, sensitive data, intellectual property, and technical and military capabilities, and undermine and disrupt U.S. foreign policy and intelligence operations. FIEs are positioning themselves to compromise or damage infrastructure critical to U.S. health, safety, and economic activity, and are attempting to influence U.S. policy and public opinion and undermine our democracy. They blend sophisticated techniques with traditional approaches while employing technical and cyber tools that are increasingly potent, widely available, and easy to use. These activities represent immediate threats to our national security, economic well-being, physical safety, democratic processes, and societal cohesion.

- The People's Republic of China (PRC) and Russia represent the most significant intelligence threats, but a range of other state and non-state actors also target the United States. Commercial entities are playing increasingly important enabling roles for FIEs.
- Our leading adversaries view themselves as already engaged in an intense, multifaceted competition with the United States. As such, their intelligence services frequently conduct more aggressive operations that fall in the "gray zone," a space between war and peace that encompasses intelligence activities that push the boundaries of accepted norms, such as covert influence, political subversion, and operations in cyberspace.
- We also see our leading adversaries cooperating more frequently with one another, enhancing the threat they pose to the United States.

The area that we need to defend is broadening as adversaries are targeting an expanding range of public and private sector entities and are employing a variety of avenues of approach, at the same time that we are using more connected devices and remote platforms that put our data, networks, and infrastructure at risk.

[1] For the purpose of this Strategy, a Foreign Intelligence Entity (FIE) is any known or suspected foreign state or non-state organization or person that conducts intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy and public opinion, disrupt U.S. systems and programs, or conduct assassination or incapacitation operations. The term includes foreign intelligence services—defined as state intelligence services—and also can pertain to international terrorists, transnational criminal organizations, foreign cyber actors, or foreign corporations or organizations (from the National Threat Identification and Prioritization Assessment, published in 2022).

- FIEs seek to collect information from virtually all U.S. Government departments and agencies, state and local governments, cleared defense contractors, commercial firms across numerous sectors, think tanks, and academic institutions. Adversaries are pursuing not only classified information but also vast troves of unclassified material that can support their political, economic, research and development (R&D), military, and influence goals, and their attempts to target U.S. persons, supply chains, and critical infrastructure.

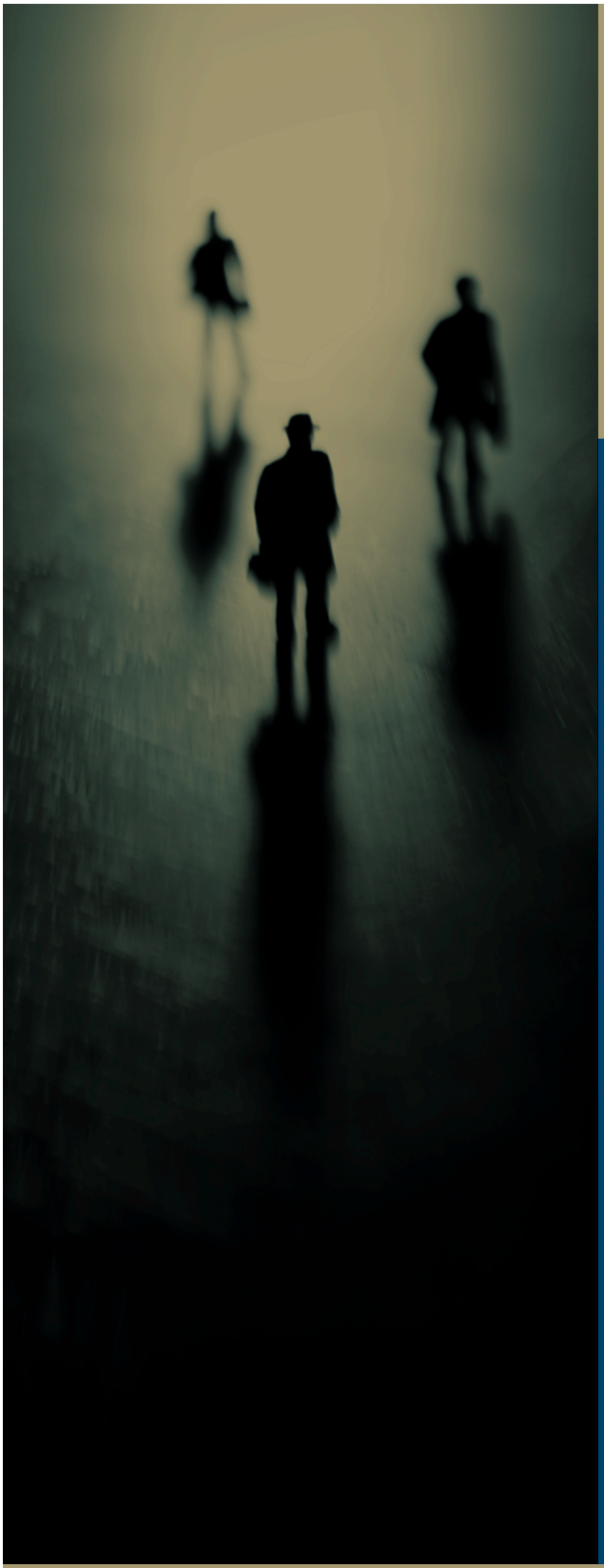
Adversaries are using cutting-edge technology—such as advanced cyber tools, biometric devices, unmanned systems, high-resolution imagery, enhanced technical surveillance equipment, commercial spyware, and Artificial Intelligence (AI)—to further their espionage, counterespionage, and influence missions. Such technology is easy to use, less expensive, and more available commercially, bringing it within reach of even relatively unsophisticated FIEs. The exponential pace of technological change complicates efforts to develop and maintain adequate defenses.

Insider threats[2] are also a vulnerability. In some cases, insiders use their authorized access, wittingly or unwittingly, to do harm to the security of the United States. In other cases, FIEs actively target, solicit, and coerce individuals to obtain information, compromise critical infrastructure, or steal our secrets.

Looking ahead, the intelligence landscape will remain dynamic and dangerous. Our current adversaries will grow more proficient and new threat actors will enter the scene, bolstered by technological advances and enhanced collaboration. Global interconnectedness will continue to leave our networks and strategic supply chains vulnerable to FIEs. The U.S. CI[3] community must work together to prioritize and integrate their efforts to counter FIE activities and disrupt and degrade their ability to harm the national security interests of the United States. ■

[2] Insider Threat: The threat that an insider will use their authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities. (Derived from National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, 21 November 2012).

[3] For the purpose of this Strategy, "counterintelligence" refers to information gathered and activities conducted to identify, assess, deceive, exploit, disrupt, neutralize, warn of, or protect against espionage, other intelligence activities, malign influence, sabotage, or assassinations conducted for or on behalf of a foreign government or elements thereof; foreign organizations, persons, or their agents; or international terrorist organizations or activities.



PILLAR ONE

Outmaneuver and Constrain Foreign Intelligence Entities

FIEs are increasingly operating in a *gray zone* between war and peace that leverages intelligence activities to push the boundaries of accepted norms without resorting to open conflict. To combat this, we must better anticipate foreign intelligence threats and work together to counter harmful intelligence activities and degrade threat actor capabilities.

GOAL 1

Detect, Understand, & Anticipate Foreign Intelligence Threats

Identify and assess new and emerging FIE threats, vulnerabilities, and changing conditions and operational environments to detect, understand, and anticipate FIE plans and activities, identify opportunities for action, and provide decision advantage.

Aggressive intelligence operations are being employed against the United States by our adversaries. Intelligence and law enforcement agencies have worked together to disrupt operations and expose foreign intelligence officers, but in today's era of strategic competition, many PRC, Russian, and Iranian intelligence activities still go undetected. To combat the expanding foreign intelligence threat more effectively, we need to know more about our adversaries' plans, intentions, techniques, activities, and vulnerabilities and better share that information with key decisionmakers. We need to focus not only on collecting secrets, but also on taking better advantage of openly available information. The CI community needs to more effectively use existing tools and develop new tools and technology to help us better understand the scope and nature of the threat. Further, we must move beyond detecting our adversaries' activities and be able to anticipate them, giving policymakers and CI and security officers the information they need to combat our adversaries in the intelligence realm.

To accomplish this goal, the U.S. Government will:

- Expand the development, adoption, and integration of innovative human, technical, and open source collection capabilities on FIEs, their proxies, and enablers to acquire unique insight and understanding into their plans, intentions, capabilities, and vulnerabilities.
- Develop and implement mechanisms to more quickly and effectively share FIE threat information across federal, state, local, tribal, and territorial governments, the private sector, and with foreign partners to provide operators, decisionmakers, and CI partners with timely and actionable insights on threats from FIEs and insiders.
- Strengthen CI collection, analysis, and reporting standards, processes, and practices to improve tradecraft and mitigate the risk of FIE manipulation and deception.

GOAL 2

Counter, Degrade, & Deter Foreign Intelligence Activities & Capabilities

Orchestrate, enable, support, and conduct coordinated offensive CI activities[4] and defensive measures[5] to counter FIE activities, degrade their capabilities, and deter future FIE threats.

FIEs have proven adept at stealing our secrets, sensitive data, and intellectual property; exerting influence over policy and public opinion; and harming U.S. persons. It is imperative that the CI community—working with our partners across all levels of government and in like-minded countries—more effectively counter and prevent these activities, using the full range of tools at our disposal to increase the costs and reduce the likelihood of success of these operations.

To accomplish this goal, the U.S. Government will:

- Leverage the full scope of CI authorities and incorporate innovative tools and techniques—including advanced information technology (IT) solutions and infrastructure, knowledge management, and AI—to enable and conduct creative offensive and defensive CI activities to identify, disrupt, and degrade our adversaries' intelligence activities.
- Discover, illuminate, and neutralize adversary FIEs' non-traditional assets and enablers to degrade their operational capabilities and hinder future activities.
- Increase integration in planning, orchestration, and execution of strategic CI activities to optimize resources and coordination to shape the adversary's information environment and disrupt the FIE threat.

[4] For the purpose of this Strategy, "offensive CI activities" are activities to identify, deceive, exploit, disrupt, and protect against the intelligence activities of foreign intelligence entities to enhance national security or provide benefit to the USG. These activities are conducted by specific departments and agencies with the requisite authorities.

[5] For the purpose of this Strategy, "defensive measures" include actions and activities designed to protect U.S. persons, organizations, and activities from the actions and activities of FIEs.

GOAL 3
Combat Foreign Intelligence Cyber Activities

Build partnerships and leverage CI and other appropriate authorities and capabilities to conduct proactive, integrated operations to identify, disrupt, degrade, neutralize, and manipulate FIE ability and willingness to use the cyber domain to threaten U.S. interests.

Cyber threats from nation states and their surrogates remain acute. FIEs use the cyber domain to undertake their full range of activities, from collection of sensitive information to disruption and destruction of networks to malign foreign influence and monitoring of dissidents. They use technical—and often commercially available—tools to compromise computer networks and mobile and connected devices. Although an increasing number of countries and non-state actors have these capabilities, we are most concerned about Russia, the PRC, Iran, and North Korea. In addition, a growing number of commercial firms are flooding the market with high-quality cyber intrusion tools, expanding the pool of FIE actors that can threaten our networks and people. We must build and better leverage partnerships, capabilities, and authorities across the federal, state, and local levels to implement innovative solutions that impose greater cost and risk to FIE cyber activities.

To accomplish this goal, the U.S. Government will:

- Foster strong partnerships across federal, state, and local government, the private sector, academia, and with foreign partners to share information, increase transparency, and build trust to gain insight into FIE cyber activities and identify opportunities for CI solutions.
- Engage federal partners and improve collaboration and coordination across disciplines to increase understanding of CI authorities and capabilities and develop tools and infrastructure that are shareable and interoperable to the extent practicable.
- Work with partners and allies to conduct integrated, scalable, prioritized, proactive CI activities to counter FIE cyber operations, introduce uncertainty, and increase costs to FIEs.

PILLAR TWO

Protect America's Strategic Advantages

Though we face tremendous challenges, there is no nation better positioned to lead with strength and purpose than the United States of America. Our strength rests upon a number of strategic advantages we must help protect and defend, including our people, our democratic institutions, our critical technology, infrastructure, and supply chains.

GOAL 4

Protect Individuals Against Foreign Intelligence Targeting & Collection

Detect, disrupt, counter, and deter FIE operations against Americans and others affiliated with the U.S. Government at home and abroad[6] and other protected individuals in the United States who may be of high interest to FIEs to safeguard their health, safety, liberty, and personal data that could be used for foreign intelligence purposes.

FIEs are targeting not only U.S. Government entities and private corporations, but also individual U.S. persons and their data; and U.S.-based foreign dissidents are increasingly among the victims of incapacitation, rendition, and assassination attempts that FIEs conduct around the world. Moreover, as part of a broader focus on data as a strategic resource, our adversaries are interested in personally identifiable information (PII) about U.S. citizens and others, such as biometric and genomic data, health care data, geolocation information, vehicle telemetry information, mobile device information, financial transaction data, and data on individuals' political affiliations and leanings, hobbies, and interests. PII—such as genomic and health care data—can be especially valuable, providing adversaries not only economic and R&D benefits, but also useful CI information, as hostile intelligence services can use vulnerabilities gleaned from such data to target and blackmail individuals. Protecting our people at home and abroad from foreign intelligence threats is a core part of the CI mission and we must adopt a unified and proactive whole-of-government approach to counter these physical and digital threats.

To accomplish this goal, the U.S. Government will:

- Expand and improve collection on FIE threats to individuals to better understand adversary plans, intentions, and capabilities, and detect activities.
- Improve timeliness and utility of actionable intelligence to support disruption efforts by law enforcement, CI operators, policymakers, commercial and academic partners, and others.
- Expand engagement with state, local, and foreign governments, private sector partners, and the U.S. public to inform decisionmaking, empower targeted individuals, and raise the risk for FIE operations in the United States.

[6] This includes American citizens, foreigners affiliated with the U.S. Government at home and abroad, and political dissidents, defectors, resettlees, or other high-risk individuals in the United States.

GOAL 5

Protect Democracy from Foreign Malign Influence

Detect, attribute, expose, and disrupt FIE malign influence efforts[7] and engage partners and policymakers to counter these operations and safeguard the integrity of and public trust in U.S. democratic institutions and processes, rule of law, and other democratic norms.

Foreign adversaries are increasing their efforts to exercise malign influence on U.S. public opinion and policy and stoke societal tensions in the United States, while burnishing their own status, denigrating the United States, and damaging our alliances and relationships around the world. Adversaries often regard such operations as a less risky and provocative way of achieving national goals and an increasing number of countries are using them. For example, in 2020 and again in 2022 the IC tracked a broader array of foreign actors taking steps to influence U.S. elections than in past election cycles. A combination of advanced techniques and tools, often fueled by technological improvements and innovations in fields such as AI and behavioral analytics, is increasing the effectiveness and persuasiveness of malign influence campaigns. Given these advancements in technology, including AI, adversaries can spread convincing messages at a quantity and pace that challenge governments' and social media firms' ability to identify, attribute, and combat them, while big-data analytics allow adversaries to more precisely target specific audiences with tailored messages. We must develop and leverage tools, technologies, and partnerships to combat adversaries' efforts to unduly influence Americans and undermine trust in our democratic institutions, norms, and rule of law.

To accomplish this goal, the U.S. Government will:

- Increase common understanding of foreign malign influence tradecraft, methods, and priorities across the spectrum of actors, targets, and platforms to enable greater detection and attribution of FIE malign influence efforts.
- Expand engagement and build robust partnerships across federal, state, local, and foreign governments and with the private sector, civil society, and academia to share information and insight, raise awareness of FIE malign influence threats, enable action, and build trust and resilience.
- Develop tailored tools and processes to increase information sharing, appropriate transparency, and collaboration to support swifter, more coordinated action to expose and disrupt FIE malign influence activities.

[7] For the purpose of this Strategy, foreign malign influence is characterized by subversive, undeclared (including covert and clandestine), coercive or criminal activities by foreign governments, non-state actors, or their proxies to affect another nation's popular or political attitudes, perceptions, or behaviors. These activities can include efforts to sow division, undermine democratic processes and institutions, and steer policy or regulatory decisions in favor of the foreign actors' strategic objectives. In this Strategy, we are focused on these actions and activities that are directed or conducted by or otherwise linked to FIEs (from the Foreign Malign Influence Lexicon, published by the National Intelligence Council, August 2022).

GOAL 6

Protect Critical Technology & U.S. Economic Security

Detect, understand, anticipate, and counter FIE attempts to exploit our open society and threats from FIE and insiders to critical U.S. technologies,[8] sensitive data, and our national innovation base[9] to protect U.S. economic and national security and competitive advantage.

Foreign economic and industrial espionage against the United States continues to represent a significant threat to America's prosperity, security, and competitive advantage. Adversaries are aggressively collecting on U.S. critical and emerging technology and are making concerted efforts to acquire the sensitive technology, intellectual property, and proprietary information that underpins U.S. economic security. FIEs use cyber espionage, embedded researchers, and front companies and investments to target innovative U.S. firms and research institutions, seeking a shortcut to build their own countries' economic and technological bases and make their firms more competitive against U.S. rivals. The PRC is the country of greatest concern in this sphere, as it targets key technology sectors and proprietary commercial and military technology from U.S. and allied companies and research institutions and uses a variety of tools, including espionage and theft, to advance its technological capabilities. We must adopt a whole-of-society approach to counter our adversaries' efforts to collect or acquire sensitive information and technology that could rapidly advance adversary capabilities in ways that could ultimately threaten the national security of the United States.

To accomplish this goal, the U.S. Government will:

- Increase analytic capacity and collection focus and refine priorities to improve detection and understanding of FIE efforts to collect on, acquire, or otherwise threaten critical U.S. technologies or sensitive data of importance to national and economic security.
- Increase CI community collaboration and build and strengthen partnerships with the private sector, academia, and other partners and allies to improve information sharing, increase threat awareness, and inform and enable targeted threat mitigation activities.
- Improve processes and procedures to identify malign foreign investment in the United States and our national innovation base and increase collaboration with key government, academic, and private sector partners to counter FIE attempts to exploit our economy.

[8] For the purpose of this Strategy, "critical U.S. technologies" includes advanced technologies that are particularly significant to U.S. national security, such as those identified by the National Science and Technology Council in its "Critical and Emerging Technologies List Update" (Feb 2022). These technologies include but are not limited to AI, quantum information technologies, biotechnology, semiconductors and microelectronics, autonomous systems and robotics, and communication and networking technologies.

[9] For the purpose of this Strategy, "national innovation base" refers to the diverse array of institutions and individuals conducting research and development, the public, academic, and private sectors that fund, mature, and field their products, and the human capital that serves as a foundation to the above through education and participation.

GOAL 7
Protect the Nation's Critical Infrastructure

Improve understanding and awareness of FIE capabilities and threats to help protect our Nation's most critical infrastructure,[10] increase resilience, deny adversary access, and deter future threats.

FIEs are laying the groundwork for potential attacks against our critical energy, communications, transportation, and financial nodes. Their capabilities and pre-positioning efforts are increasing the risk of a large-scale disruption during periods of conflict or tension, which could include degraded military readiness, major economic losses, loss of life, or eroded confidence in key institutions. In particular, a well-targeted FIE attack on critical infrastructure that causes lasting disruption could have a catastrophic economic impact—not only on the entities directly affected but also on all the downstream users who rely on that infrastructure—and result in billions of dollars in losses. U.S. critical infrastructure systems are often interdependent, meaning that an attack on one system could cause outages in other systems or spread to other geographic areas. Our adversaries' efforts are likely aimed at influencing or coercing U.S. decisionmakers in a time of crisis by holding critical infrastructure at risk of disruption. We must work collaboratively across public and private sectors to share information, identify threats, and enable action by critical infrastructure owners and operators to reduce vulnerabilities and counter threats.

To accomplish this goal, the U.S. Government will:

- Develop and maintain collaborative and scalable partnerships with the private sector, federal, state, local, tribal, and territorial government departments and agencies, and other allies to improve coordination and collaboration, build trust, and enable action.
- Facilitate information sharing and data integration across government and with the private sector to gain deeper insight into interdependencies between sectors, vulnerabilities, and threats from FIE and insiders to our most critical infrastructure.
- Develop and mature innovative analytic tools and tradecraft to better identify, understand, and anticipate FIE operations and activities affecting U.S. critical infrastructure.

[10] For the purpose of this Strategy "critical infrastructure" includes assets, networks, and systems—whether physical or virtual—which are so essential that their continued safe operation is vital to public confidence and the security, safety, prosperity, and well-being of the nation and its people.

GOAL 8
Reduce Risks to Key U.S. Supply Chains

Detect, understand, anticipate, and expose threats from FIE and insiders to key U.S. supply chains and inform stakeholders to mitigate risk, reduce opportunities for exploitation and compromise, and deter future threats.

The exploitation of key U.S. supply chains[11] by foreign adversaries, especially when executed in concert with cyber intrusions and insider threat activities, represents a complex and growing threat to strategically important U.S. economic sectors and critical infrastructure. Foreign adversaries are attempting to access our Nation's key supply chains at multiple points—from concept to design, manufacture, deployment, and maintenance—by a variety of means. Successful supply chain compromises could allow an adversary to extract intellectual property, sensitive government data, and PII. It could also allow an adversary to surveil, deny, disrupt, or otherwise degrade a component, system, or service, thereby adversely affecting critical industrial control systems, services, and products. For example, during the last decade, state-sponsored hackers have compromised software and IT service supply chains, facilitating espionage and sabotage operations and potentially allowing for prepositioning for warfighting. We must better integrate efforts to manage risks and expand efforts to build strong partnerships and share information to mitigate threats.

To accomplish this goal, the U.S. government will:

- Improve analytic tradecraft, increase data sharing, and deepen integration of existing supply chain risk management efforts across the U.S. government to build greater expertise and understanding of supply chain threats and vulnerabilities.
- Expand and prioritize collection on FIE plans, intent, access, and capabilities to exploit, disrupt, or sabotage key U.S. supply chains to better detect and anticipate such threats.
- Increase engagement and partnership with federal, state, local, and foreign government partners, private industry, and the public to share information, build trust, and gain insight into current supply chain vulnerabilities and future areas of investment to better understand, anticipate, and mitigate threats.

[11] For the purpose of this Strategy, supply chains are networks of people, processes, technology, information, and resources that deliver a product or service. For the purposes of this Strategy "key U.S. supply chains" includes those supply chains that involve companies, materials, and systems strategically placed to provide goods and services vital to our national and economic security, including those supply chains referenced in Executive Order 14017, "America's Supply Chains," 24 February 2021.

PILLAR THREE

Invest in the Future

We must invest in the future to develop the capability and capacity to meet these challenges and protect America's strategic advantage. We must reinvigorate our CI community, build and enable strong partnerships, and increase collaboration to build resilience against current and future foreign intelligence threats.

GOAL 9

Build Counterintelligence Capabilities, Partnerships, & Resilience

Drive investment and innovation in the CI community to build the skills, expertise, capabilities, and authorities, and advance partnerships to increase awareness, improve resilience, and achieve enduring superiority over our FIE adversaries.

Building the capabilities of the U.S. CI community to more effectively combat the myriad intelligence threats facing the country and better posture itself for the future will require significant investment in both people and technology. Many of our adversaries see the United States as their primary intelligence target, so we need a strong CI cadre steeped in subject-area expertise to tackle the threat. Our adversaries take a whole-of-government approach to their activities against the United States so we need to ensure that our agencies' roles, responsibilities, and authorities are clear and do not create seams in which our adversaries can operate. Our adversaries are working against a broad range of targets—including our allies overseas, state and local governments, the private sector, and academia—so we all must work together to keep our secrets, people, data, and infrastructure secure.

To accomplish this goal, the U.S. Government will:

- Drive investment in innovative technologies and integrated solutions and leverage existing research platforms to close key CI gaps, strengthen capabilities, and outpace rapid changes in the CI environment at home and abroad.
- Recruit, hire, train, and retain a trusted and diverse CI workforce comprised of officers with the necessary knowledge, skills, and specialized expertise to meet current and future threats and outperform our adversaries.
- Align, reconcile, and supplement individual federal department, agency, and organizations' CI authorities as needed to eliminate gaps and strengthen and broaden U.S. Government capability to defeat FIE threats to the nation.
- Expand and strengthen partnerships and collaboration across the federal government and with state, local, foreign, and private sector partners to increase awareness and information sharing, deepen understanding, and bolster the nation's resilience against FIE threats.

Conclusion

As we look to the future, U.S. national and economic security interests will continue to face formidable foreign intelligence threats. Countering the wide array of evolving threats will require a whole-of-society approach that increases coordinated actions by federal, state, local, tribal, and territorial governments and increases engagement and cooperation with our allies and partners—including the private sector, academia, and an informed public. This strategy provides the foundation to effectively drive an integrated and coordinated response to our most significant FIE threats. Effective implementation of this strategy will be key to our success. U.S. Government departments and agencies shall align their CI priorities and resources to the goals and objectives of this strategy, work together to achieve them, and measure and evaluate their progress toward the strategic outcomes identified herein. ■