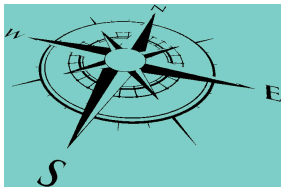
National Counterintelligence Strategy of the United States of America 2020-2022

This National Counterintelligence Strategy of the United States of America, 2020-2022 presents a new perspective on how to effectively address foreign intelligence threats as a nation. Five strategic objectives encompass the most critical areas where foreign intelligence services are targeting the United States: Critical Infrastructure; Key U.S. Supply Chains; the U.S. Economy; American Democracy; and Cyber and Technical Operations.

It is essential that we engage and mobilize all elements of United States society and fully integrate sound counterintelligence and security procedures into our business practices, and strengthen our networks against attempts by foreign threat actors or malicious insiders to steal or compromise our sensitive data, information, and assets.

Contents



Office of the Director of National Intelligence (DNI)

Stakeholder(s):

William R. Evanina :
Director, National Counterintelligence and Security Center

Vision

The United States is protected against espionage and other damaging intelligence activities.

Mission

To anticipate and deter threats from foreign intelligence services, as well as state and non-state actors.

Values

Intelligence

Security

Innovation

Action

1. Critical Infrastructure

Protect the Nation's Critical Infrastructure

Stakeholder(s)

National Critical Functions :
"National Critical Functions are the functions of government and the private sector produced by infrastructure so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." DHS/CISA Information Paper: National Critical Functions: An Evolved Lens for Critical Infrastructure Security and Resilience, 30 April 2019.

Protect the nation's civil and commercial, defense mission assurance, and continuity of government infrastructure from foreign intelligence entities seeking to exploit or disrupt national critical functions. Foreign intelligence entities are developing the capacity to exploit, disrupt, or degrade critical infrastructure worldwide. Their efforts likely are aimed at influencing or coercing U.S. decision makers in a time of crisis by holding critical infrastructure at risk of disruption. The decentralized and digital nature of critical infrastructure worldwide creates vulnerabilities that could be exploited by foreign intelligence entities, and they also are targeting the facilities and networks that underpin global energy and financial markets, telecommunications services, government functions, and defense capabilities. Disruption of U.S. critical infrastructure could undermine our nation's security, economy, public health and safety in a variety of ways. For example, adversaries seeking to cause societal disruption in the United States could attack the electrical grid causing a large-scale power outage that affects many aspects of daily life. Additionally, foreign adversaries could disrupt the U.S. economy by interfering with the ability of individuals and businesses to conduct financial transactions. We must work with our allies and partners to identify and mitigate foreign intelligence threats to critical infrastructure upon which our collective national and economic security depends. To meet this objective, the U.S. Government will:

1.1. Information Exchanges

Expand critical infrastructure information exchanges with federal departments and agencies; with state, local, tribal, and territorial governments; and with private sector partners, and allies.

The U.S. Government will enhance the capability to share threat, incident, vulnerability and risk data with our partners, including providing critical infrastructure owners and operators with actionable information and security best practices.

Stakeholder(s):

State Governments

Local Governments

Tribal Governments

Territorial Governments

Private Sector Partners

Allies

Infrastructure Owners

Infrastructure Operators

1.2. Community

Develop, train, and retain a community of officers across government who can identify and counter threats to U. S. critical infrastructure.

Development of this community will provide a dedicated cadre of critical infrastructure subject matter experts to enable timely warning, provide increased threat awareness and information sharing, and develop more agile responses to foreign intelligence threats.

Stakeholder(s):

Infrastructure Officers

1.3. Analytic Tools

Develop new analytic tools to improve threat warning and enable offensive and defensive operations.

The U.S. Government will leverage existing analytic tools and develop new tools to help analysts and operators visualize threats and vulnerabilities, and provide data to help officers prioritize our limited counterintelligence resources against the highest priority threats

2. Supply Chains

Reduce Threats to Key U.S. Supply Chains

Stakeholder(s)

Governments **American Industry**

Reduce threats to key U.S. supply chains to prevent foreign attempts to compromise the integrity, trustworthiness, and authenticity of products and services purchased and integrated into the operations of the U.S. Government, the Defense Industrial Base, and the private sector. The exploitation of key supply chains 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, integration, deployment, and maintenance—by inserting malware into important information technology networks and communications systems. The increasing reliance on foreign-owned or controlled hardware, software, or services as well as the proliferation of networking technologies, including those associated with the Internet of Things, creates vulnerabilities in our nation's supply chains. By exploiting these vulnerabilities, foreign adversaries could compromise the integrity, trustworthiness, and authenticity of products and services that underpin government and American industry, or even subvert and disrupt critical networks and systems, operations, products, and weapons platforms in a time of crisis. We must elevate the role of supply chain security in the acquisition process. To meet this objective, the U.S. Government will:

2.1. Threats

Enhance capabilities to detect and respond to supply chain threats.

We will develop access to new sources of information and increase the analytic capacity to understand and assess foreign intent and capability to exploit U.S. supply chains. We will also implement new processes to identify suspect or high risk vendors, products, software and services that pose a risk to our economic and national security.

Stakeholder(s):

Vendors **Service Providers**

Software Providers

2.2. Integrity & Security

Advance supply chain integrity and security across the federal government.

We will integrate Supply Chain Risk Management capabilities and processes consistent with industry best practices into the operations of the federal government to safeguard the technology and services that are procured and deployed. We will create a supply chain risk assessment shared repository, address deficiencies in the federal acquisition process, and seek more streamlined authorities to exclude high risk vendors.

Stakeholder(s):

Vendors

2.3. Outreach

Expand outreach on supply chain threats, risk management, and best practices.

Through expanded outreach and sustained engagement, we will establish and deepen partnerships with state, local, tribal, and territorial governments, and the private sector, and share supply chain threat information and mitigation measures with our partners, especially in U.S. critical infrastructure sectors.

Stakeholder(s):

State Governments

Local Governments

Tribal Governments

Territorial Governments

Private Sector

3. Economy

Counter the Exploitation of the U.S. Economy

Stakeholder(s)

American companies

Counter the exploitation of the U.S. economy to protect America's competitive advantage in world markets and our technological leadership, and to ensure our economic prosperity and security. Many countries target the United States because it is a global center for high-technology research, technology and innovation. Foreign intelligence entities have embedded themselves into U.S. national labs, academic institutions, and industries that form America's national innovation base. They have done this to acquire information and technology that is critical to the growth and vitality of the U.S. economy. Adversaries use front companies, joint ventures, mergers and acquisitions, foreign direct investment, and talent recruitment programs to gain access to and exploit U.S. technology and intellectual property. They also influence and exploit U.S. economic and fiscal policies and trade relationships. These activities have cost the United States hundreds of billions of dollars. The theft of our most sensitive technologies, research and intellectual property harms U.S. economic, technological, and military advantage in the world. It puts at risk U.S. innovation and the competitiveness of American companies in world markets. To meet this objective, the U.S. Government will:

3.1. Detection

Improve detection of foreign threats to our national innovation base.

We will develop access to new sources of information and increase analytic capacity to understand and assess these threats.

3.2. Awareness

Broaden awareness of foreign intelligence threats to the U.S. Economy.

We will share threat information and mitigation strategies with U.S. academia, key industries and critical infrastructure sectors.

Stakeholder(s):

U.S. Academia

Critical Infrastructure Sectors

Key Industries

3.3. Foreign Investments

Identify and counter foreign investments in the United States that pose a national security threat.

We will work with the private sector to develop better procedures to track foreign investment in the United States and better understand, share, and potentially mitigate counterintelligence issues arising from these investments.

Stakeholder(s):

Private Sector

4. Democracy

Defend American Democracy against Foreign Influence

Defend the United States against foreign influence to protect America's democratic institutions and processes, and preserve our culture of openness. Foreign intelligence entities are conducting influence campaigns in the United States to undermine confidence in our democratic institutions and processes, sow divisions in our society, exert leverage over the United States and weaken our alliances. These campaigns are designed, for example, to sway public opinion against U.S. Government policies or in favor of foreign agendas, influence and deceive key decision makers, alter public perceptions, and amplify conspiracy theories. These campaigns can include the targeting of our democratic and electoral processes using influence operations that can be long in duration, have broad strategic implications, and include activities that are covert, overt, and illegal. Our adversaries regard deception or manipulation of the views of U.S. citizens and policymakers to be an effective, inexpensive, and low-risk method for achieving their strategic objectives. Our adversaries are using a range of communications media to enable their covert influence campaigns. Using false U.S. personas, foreign intelligence entities develop and operate social media sites and other forums to draw the attention of U.S. audiences, spread misinformation, and deliver divisive messages. To meet this objective, the U.S. Government will:

4.1. Capabilities & Activities

Advance our counterintelligence capabilities and activities to detect, deter and counter foreign influence activities.

We will strengthen and integrate our processes and capabilities to identify and address knowledge gaps and mitigate threats.

4.2. U.S. Partnerships

Strengthen partnerships across U.S. Government departments and agencies; with state, local, tribal, and territorial governments; and with the private sector.

We will strengthen partnerships especially with social media providers, technology companies, and academia – to raise awareness of foreign influence activity, better understand the threat, and provide timely, substantive warning of foreign intentions to interfere with or influence U.S. policy, officials, or the American public.

Stakeholder(s):

State Governments

Local Governments

Tribal Governments

Territorial Governments

Private Sector

Social Media Providers

Technology Companies

Academia

U.S. Officials

American Public

4.3. Foreign Partnerships

Deepen existing and develop new foreign partnerships.

We will strengthen collaboration with our foreign partners to raise awareness of foreign influence activity, share lessons learned and best practices, and inform decisions to counter threats.

Stakeholder(s):

Foreign Partners

5. Cyber & Technical Operations

Counter Foreign Intelligence Cyber and Technical Operations

Counter foreign intelligence cyber and technical operations that are harmful to U.S. interests. Our foreign adversaries are capable of conducting cyber espionage and technical operations against U.S. interests around the world and they continue to develop new and more effective capabilities in these areas. Readily available and advanced cyber and technical surveillance tools offer threat actors a relatively low-cost, efficient, deniable, and high-yield means of accomplishing their goals. The development of next generation technologies such as the Internet of Things, fifth generation (5G) cellular communications technology, quantum computing, and artificial intelligence will continue to present new opportunities for foreign intelligence entities to collect intelligence and conduct cyber operations against the United States and its allies. The U.S. Government must pursue a more integrated cyber counterintelligence posture to defend against hybrid attack methods that involve supply chain, cyber, technical means and insider enabled attacks. This will require leveraging innovative technological advancements; recruiting, developing and retaining technical experts in the cyber, counterintelligence and security disciplines; and stronger partnerships among the federal, state and local governments, and the private sector. To meet this objective, the U.S. Government will:

5.1. Integration

Advance the integration of the counterintelligence, security and cyber communities to better detect, deter, and counter the threats from foreign intelligence cyber actors.

By more effectively integrating these disciplines we will deepen our understanding of our adversaries' cyber and technical threat intent and capability, as well as our own vulnerabilities. We will work across the whole-of-government, the private sector, and the American public to enhance mechanisms for information sharing and implement more effective defenses.

Stakeholder(s):

Counterintelligence Community

Security Community

Cyber Community

Private Sector

American Public

5.2. Expertise

Develop, train, and retain a cadre of cyber counterintelligence and technical security experts.

Development of this national security community will allow for more rapid recognition of threats and vulnerabilities, and more agile responses and integrated approaches to counter adversary cyber and technical activities.

Stakeholder(s):

Cyber Counterintelligence Security Experts

Technical Security Experts

5.3. Toolkit

Enhance our cyber counterintelligence toolkit.

We will work to develop and acquire new capabilities to track and counter foreign cyber and technical operations against the United States and leverage partnerships with the private sector to develop effective countermeasures.

Stakeholder(s):

Private Sector

Implementation

Stakeholder(s)

U.S. Government Departments **U.S. Government Agencies**

IMPLEMENTING THE NATIONAL COUNTERINTELLIGENCE STRATEGY — 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 threats and keeping the American public informed is a core obligation of the entire U.S. Government. However, we cannot address these national security challenges alone. It will require a whole-of-society approach that not only relies on coordinated actions by federal, state, local, tribal, and territorial governments but also on the support from allies and partners, the private sector and the active engagement of an informed public. This Strategy provides the foundation to effectively integrate counterintelligence practices through partnerships, information sharing, and innovation. Additionally, U.S. Government departments and agencies are responsible for aligning their counterintelligence priorities and resources to the objectives within this Strategy, and measuring progress towards achieving those objectives. Implementation efforts should be guided by the following:

Actionable Intelligence

Enable a common understanding of foreign intelligence threats and provide timely, substantive, and actionable intelligence to strengthen the nation's ability to mitigate and counter threats.

Partnerships and Information Sharing to enable a common understanding of foreign intelligence threats and provide timely, substantive, and actionable intelligence to strengthen the nation's ability to mitigate and counter threats. Increased collaboration among counterintelligence, industry, and academic leaders will deepen our understanding of foreign adversary intentions and capabilities and foster joint capabilities to detect and defend against threats.

Innovation

Innovate to develop and deploy critical technologies and solutions to advance our counterintelligence capabilities.

We will develop counterintelligence information repositories that enable indications and warnings and mitigations of potential foreign threats to the United States. Additionally, we will develop a more agile and integrated technical countermeasures program that can keep pace with rapid technological advances.

Strategic Alignment

Align Strategies, Plans, and Guidance to the five objectives within this Strategy to enable stronger integration of our collective counterintelligence efforts.

Resources

Identify Resource Requirements to ensure counterintelligence mission activities related to these objectives are adequately reflected and prioritized within the planning, programming, and budgeting cycle.

Evaluation

Evaluate Performance to measure progress against this Strategy's objectives.

Administrative Information

Start Date: 2020-01-01
End Date: 2022-12-31

Publication Date: **2020-05-05**
Source: https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf

Submitter:

Given Name: Owen
Surname: Ambur
Email: Owen.Ambur@verizon.net
Phone: