National Counterintelligence Strategy

of the United States of America 2020-2022

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

NOTE: This *National Counterintelligence Strategy of the United States of America 2020-2022*, fulfills the requirement of the Counterintelligence Enhancement Act of 2002. This *Strategy* was approved by the Director of the National Counterintelligence and Security Center in August 2019, and sent to the President for signature. It was approved by the President on December 25, 2019 and signed on January 7, 2020.

THE WHITE HOUSE

WASHINGTON

January 7, 2020

Protecting our Nation's security and continuing to enhance the prosperity of our citizens are my top priorities. Ensuring that the United States is protected against espionage and other damaging intelligence activities conducted by our foreign adversaries is essential to meeting those goals.

The Nation faces an expanding array of foreign intelligence threats by adversaries who are using increasingly sophisticated methods to harm the United States. Russia remains a significant intelligence threat to United States interests - employing aggressive acts to instigate and exacerbate tensions and instability in the United States, including interfering with the security of our elections. A more powerful and emboldened China is increasingly asserting itself by stealing our technology and intellectual property in an effort to erode United States economic and military superiority. Regional adversaries and ideologically motivated entities, such as hackers and public disclosure organizations, pose a growing threat to the United States. These actors are increasingly able to advance their goals due to the proliferation of more effective and commercially available cyber and surveillance technologies.

The *National Counterintelligence Strategy* explains how my Administration will:

- Protect the American people, the Homeland and the American way of life from foreign intelligence services that seek to harm us;
- Promote American prosperity by protecting our economy from foreign adversaries who seek to steal our technology and intellectual property; and
- Preserve peace and security by going on the offensive against aggressive foreign intelligence services that work against democracy, United States allies, and our national security priorities.

This *Strategy* demonstrates my commitment to strengthening America's counterintelligence and security capabilities and securing America from foreign intelligence threats. In order to accomplish these objectives, the United States Government must work together with private industry and the American public as partners in this effort.

Office of the Director of National Intelligence
Director of the National Counterintelligence and Security Center
Washington, DC 20511

The United States is facing increasingly aggressive and complex threats from foreign intelligence services, as well as state and non-state actors. To anticipate and deter these threats, the U.S. Government continues to address its fundamental, core counterintelligence missions: identifying, assessing, and neutralizing foreign intelligence activities and capabilities in the United States; mitigating insider threats, countering espionage and assassination attempts by foreign intelligence services from occurring on U.S. soil and abroad; and protecting U.S. sensitive and classified information and sensitive facilities from technical penetrations or espionage.

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.

This *Strategy* identifies areas where foreign threat actors could cause serious damage to our national and economic security and where we need to invest attention and resources. It also describes activities currently being undertaken, or planned, to counter threats from foreign adversaries.

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.

My office is committed to working with federal, state and local governments, the private sector, universities, as well as with our foreign partners to counter the threats posed by foreign adversaries. Together we will build on past successes to safeguard our nation's most sensitive information and assets.

William R. Evanina
Director, National Counterintelligence and Security Center

CONTENTS

THE FOREIGN INTELLIGENCE THREAT LANDSCAPE

Threats to the United States posed by foreign intelligence entities[1] are becoming more complex, diverse, and harmful to U.S. interests. Foreign intelligence actors—to include nation-states, organizations, and individuals—are employing innovative combinations of traditional spying, economic espionage, and supply chain and cyber operations to gain access to critical infrastructure,[2] and steal sensitive information, research, technology, and industrial secrets. They are conducting malicious influence campaigns using cyber operations, media manipulation, covert operations, and political subversion to sow divisions in our society, undermine confidence in our democratic institutions, and weaken our alliances. Foreign threat actors have become more dangerous because, with ready access to advanced technology, they are threatening a broader range of targets at lower risk. In aggregate, three principal trends characterize the current and emerging counterintelligence[3] environment:

The number of actors targeting the United States is growing. Russia and China operate globally, use all instruments of national power to target the United States, and have a broad range of sophisticated intelligence capabilities. Other state adversaries such as Cuba, Iran, and North Korea; non-state actors such as Lebanese Hizballah, ISIS, and al-Qa'ida; as well as, transnational criminal organizations and ideologically motivated entities such as hacktivists, leaktivists, and public disclosure organizations, also pose significant threats. Additionally, foreign nationals with no formal ties to foreign intelligence services steal sensitive data and intellectual property.

---

[1] The term "foreign intelligence entity" refers to a 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, or disrupt U.S. systems and programs. It includes foreign intelligence services—defined as state intelligence services—and can also pertain to international terrorists, transnational criminal organizations, foreign cyber actors, or foreign corporations or organizations. – *2018 National Threat Identification and Prioritization Assessment*.

[2] Critical infrastructure represents systems and assets—both physical and virtual—that are so vital to the nation that their incapacity or destruction would have a debilitating impact on our national security, economic integrity, and public health or safety (USA Patriot Act of 2001, section 1016 (e)). The sixteen U.S. critical infrastructure sectors are: Chemical; Dams; Financial Services; Information Technology; Commercial Facilities; Defense Industrial Base; Food and Agriculture; Nuclear Reactors, Materials, and Waste; Communications; Emergency Services; Government Facilities; Transportation Systems; Critical Manufacturing; Energy; Health Care and Public Health; and Water and Wastewater Systems. In January 2017, the U.S. election infrastructure was designated by the Department of Homeland Security as a subsector of the existing Government Facilities Sector.

[3] Counterintelligence: Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities. – Executive Order 12333, as amended, United States Intelligence Activities.

Threat actors have an increasingly sophisticated set of intelligence capabilities at their disposal and are employing them in new ways to target the United States. The global availability of technologies with intelligence applications—such as biometric devices, unmanned systems, high resolution imagery, enhanced technical surveillance equipment, advanced encryption, and big data analytics—and the unauthorized disclosures of U.S. cyber tools have enabled a wider range of actors to obtain sophisticated intelligence capabilities previously possessed only by well-financed intelligence services. These technologies have opened up new opportunities for adversaries to use information as a strategic resource in achieving their economic security aims, and exert leverage over their competitors.

Threat actors are using these capabilities against an expanded set of targets and vulnerabilities. Foreign intelligence entities are targeting most U.S. government departments and agencies—even those without a national security mission—as well as national laboratories, the financial sector, the U.S. industrial base and other private sector and academic entities. Some adversaries are conducting intelligence operations to exploit, disrupt, and damage U.S. and allied critical infrastructure and military capabilities during a crisis. These actors also seek to influence and exploit U.S. economic interests through a variety of intelligence activities. U.S. and allied public opinion is also a target of foreign influence activities.

The ever-changing technology landscape is likely to accelerate these trends, threatening the security and economic well-being of the American people and eroding the United States' economic, military, and technological advantage around the globe. Emerging technologies such as artificial intelligence, quantum computing, nanotechnology, advanced materials, improved encryption, robotics, and the Internet of Things will likely enable our adversaries to develop sophisticated intelligence capabilities to target the United States and make it more difficult to defend against their activities.

These intelligence activities put U.S. critical infrastructure at risk, and could jeopardize U.S. military operations and capabilities, diminish our advantage in multiple domains— including space—and undermine the integrity, trustworthiness, and authenticity of American products and services. They also expose the United States to strategic risks in areas where the counterintelligence community alone is not sufficiently positioned to mitigate them. Accordingly, we must marshal the U.S. Government, public and private partners, foreign allies and institutions, and the American public to adopt a more proactive counterintelligence and security posture and deter our adversaries from conducting intelligence activities that put our people, economy, information, systems, and intellectual property at risk.

STRATEGIC OBJECTIVES

PROTECT THE NATION'S CRITICAL INFRASTRUCTURE

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.

REDUCE THREATS TO KEY U.S. SUPPLY CHAINS

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.

COUNTER THE EXPLOITATION OF THE U.S. ECONOMY

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.

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.

COUNTER FOREIGN INTELLIGENCE CYBER AND TECHNICAL OPERATIONS

Counter foreign intelligence cyber and technical operations that are harmful to U.S. interests.

STRATEGIC OBJECTIVES

The *Strategy* focuses on five objectives:

- **Protect the Nation's Critical Infrastructure**
- **Reduce Threats to Key U.S. Supply Chains**
- **Counter the Exploitation of the U.S. Economy**
- **Defend American Democracy against Foreign Influence**
- **Counter Foreign Intelligence Cyber and Technical Operations**

These objectives are not necessarily provided in order of priority. Rather, they represent areas where foreign intelligence threats are most damaging to our national security interests and where investments in capabilities and resources are necessary to advance our counterintelligence and security posture.

The U.S. Government will continue to address core and continuing counterintelligence missions: identifying, assessing, and neutralizing foreign intelligence activities and capabilities in the United States and abroad and protecting U.S. national secrets (i.e. sensitive and classified information) and sensitive facilities from technical penetrations or espionage. These missions include countering espionage and assassination attempts by foreign intelligence services from occurring on U.S. soil, and mitigating insider threats.

To meet the increasing challenges posed by foreign intelligence actors, the United States will need to employ whole-of-government counterintelligence and security approaches that effectively integrate offensive and defensive measures and leverage all instruments of American power. The United States also must continue building the foundational knowledge necessary to understand the structures, capabilities, and resources of adversarial intelligence services, as well as counter the traditional espionage activities of our top adversaries.

PROTECT THE NATION'S CRITICAL INFRASTRUCTURE

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.[4]

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:

- **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.

- **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.

- **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

4 "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.

REDUCE THREATS TO KEY U.S. SUPPLY CHAINS

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:

- **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.

- **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.

- **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.

COUNTER THE EXPLOITATION OF THE U.S. ECONOMY

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:

- **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.

- **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.

- **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.

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:

- **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.

- **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.

- **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.

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:

- **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.

- **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.

- **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.

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:

- **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.

- **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.

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

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

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


Lincoln Sea
Beaufort Sea
Queen Elizabeth
GREENLAND (Denmark)
Greenland Sea
Baffin Bay
Davis Strait
Nunavut Territory
ALASKA (U.S.A.)
Anchorage
Denmark Strait
ICELAND
Reykjavik
Norwegian Sea
NORWAY
Oslo
C A N A D A
Hudson Bay
Labrador Sea
Gulf of Alaska
Rocky Mountains
Quebec
Island of Newfoundland
North Sea
UNITED KINGDOM
IRELAND
Dublin
London
FRANCE
Paris
Edmonton
Vancouver
Calgary
Regina
Winnipeg
Seattle
Portland
Ottawa
Montreal
Toronto
Detroit
Boston
Nova Scotia
Salt Lake City
Denver
Chicago
New York
Philadelphia
Baltimore
Washington
Kansas City
St. Louis
Sacramento
San Francisco
Los Angeles
San Diego
Mexicali
El Paso
Dallas
Houston
New Orleans
Memphis
Atlanta
San Antonio
UNITED STATES OF AMERICA
NORTH ATLANTIC OCEAN
PORTUGAL
Lisbon
Porto
Madrid
SPAIN
Barcelona
Sevilla
Algiers
Oran
Constantine
Rabat
Casablanca
Fes
Marrakesh
MOROCCO
ALGERIA
TUNISIA
WESTERN SAHARA
Monterrey
Gulf of Mexico
Miami
BAHAMAS
Havana
CUBA
MEXICO
Tampico
Guadalajara
Merida
Cancun
Mexico
Acapulco
DOMINICAN REP.
HAITI
Port-au-Prince
Santo-Domingo
ST KITTIS AND NEVIS
ANTIGUA AND BARBUDA
DOMINICA
TROPIC OF CANCER
NORTH PACIFIC OCEAN
BELIZE
JAMAICA
HONDURAS
GUATEMEALA
EL SALVADOR
NICARAGUA
Caribbean Sea
ST LUCIA
BARBADOS
ST VINCENT AND THE GRENADINES
GRENADA
TRINIDAD AND TOBAGO
COSTA RICA
PANAMA
Maracaibo
Merida
Caracas
VENEZUELA
Georgetown
Paramaribo
GUYANA
FRENCH GUYANA (France)
Medellin
Bogota
Cali
COLOMBIA
Boa Vista
SURINAME
MAURITANIA
MALI
NIGER
CAPE VERDE
Nouakchott
Dakar
SENEGAL
Praia
GAMBIA
Bamako
BURKINA
Niamey
GUINEA-BISSAU
GUINEA
Ouagadougou
Conakry
BENIN
NIGERIA
Abuja
Freetown
SIERRA LEONE
Monrovia
COTE DIVOIRE
GHANA
Accra
Lagos
Yamous
LIBERIA
Abidjan
TOGO
EQUAT. GUINEA
SAO TOME AND PRINCIPE
GABON
ECUADOR
Quito
Guayaquil
Belem
Sao Luis
Fortaleza
Natal
Recife
Manaus
Teresina
Iquitos
PERU
Amazon Basin
Porto Velho
Trujillo
Lima
Cusco
Aracaju
Salvador
BRAZIL
Cuiaba
Brasilia
La Paz
BOLIVIA
Sucre
Arica
Iquique
Belo Horizonte
Vitoria
Rio de Janeiro
Antofagasta
PARAGUAY
Sao Paulo
Asuncion
Curitiba
Florianopolis
TROPIC OF CAPRICORN
SOUTH ATLANTIC OCEAN
Cordoba
Santa Fe
Porto Alegre
Valparaiso
Santiago
Rosario
URUGUAY
Montevideo
Buenos Aires
La Plata
Concepcion
CHILE
Bahia Blanca
ARGENTINA
SOUTH PACIFIC OCEAN
Patagonia
Strait of Magellan
Punta Arenas
Cape Horn
Falkland Islands (U.K.)
Amundsen Sea
Bellingshausen Sea
Weddell Sea
A N T A R


ARCTIC OCEAN
Franz Josef Land (Russia)
North Land (Russia)
Svalbard (Norway)
New Zemlya (Russia)
Kara Sea
Laptev Sea
New Siberian Islands
Barents Sea
North Cape
Taymyr Peninsula
East Siberians
Central Siberian Plateau
West Siberian Plain
RUSSIAN FEDERATION
Ural Mountains
Scandinavia
FINLAND
SWEDEN
Helsinki
Stockholm
ESTONIA
LATVIA
LITHUANIA
St. Petersburg
Arkhangelsk
Yaroslavl
Nizhniy Novgorod
Perm
Yekaterinburg
Tomsk
Krasnoyarsk
Moscow
Chelyabinsk
Omsk
Novosibirsk
Minsk
Tula
Ufa
Barnaul
Sea of Okhotsk
Bering
POLAND
BELARUS
Berlin
Warsaw
Penza
Samara
Orenburg
Astana
Irkutsk
Sakhalin
Kiev
CZECH REP.
UKRAINE
Voronezh
SLOVAKIA
Volgograd
KAZAKHSTAN
Ulan Bator
Khabarovsk
AUSTRIA
HUNGARY
MOLDOVA
Rostov-na-Donu
Astrakhan
MONGOLIA
Harbin
CROATIA
ROMANIA
Belgrad
SERBIA
Bucharest
Black Sea
Gobi Desert
BULGARIA
UZBEKISTAN
Almaty
Bishkek
Vladivostok
Shenyang
Sofia
GEORGIA
KYRGYZSTAN
Istanbul
ARMENIA
AZERB.
TURKMENISTAN
Tashkent
Beijing
Dalian
NORTH KOREA
Sea of Japan
JAPAN
Ankara
Ashgabat
Tianjin
Pyongyang
Athens
TURKEY
Dushanbe
TAJIKISTAN
Seoul
Mashhad
Taiyuan
Jinan
Zibo
SOUTH KOREA
GREECE
Tehran
Tokyo
MALTA
CYPRUS
SYRIA
Kabul
Yellow Sea
Hiroshima
Osaka
Mediterranean Sea
LEBANON
Damascus
Baghdad
Qom
IRAN
AFGHANISTAN
Islamabad
Himalaya
CHINA
Xi'an
Tripoli
ISRAEL
IRAQ
Isfahan
Faisalabad
Lahore
Chengdu
Wuhan
Nanjing
Shanghai
Alexandria
JORDAN
Cairo
KUWAIT
PAKISTAN
NEPAL
East China Sea
LIBYA
SAUDI ARABIA
New Delhi
Kathmandu
BHUTAN
NORTH PACIFIC OCEAN
EGYPT
Medina
BAHRAIN
Riyadh
QATAR
Abu Dhabi
Karachi
Hyderabad
BANGLADESH
Taipei
U.A.E.
Muscat
Calcutta
Dakka
MYANMAR (BURMA)
Canton
Shenzhen
Hong Kong
TAIWAN
Jeddah
Mecca
Arabian Peninsula
OMAN
INDIA
LAOS
Hanoi
Bombay (Mumbai)
Naypyidaw
Vientiane
CHAD
SUDAN
YEMEN
Hyderabad
Rangoon
THAILAND
VIETNAM
Khartoum
ERITREA
Sanaa
Arabian Sea
Manila
Bangkok
CAMBODIA
South China Sea
Bangalore
Madras
Phnom Penh
PHILIPPINES
MARSHALL ISLANDS
Ndjamena
DJIBOUTI
Ho Chi Minh City
Addis Ababa
SOMALIA
SRI LANKA
Colombo
Koror
FEDERATED STATES OF MICRONESIA
CENDRAL AFRICAN REP.
SOUTH SUDAN
Palikir
Majuro
Bangui
ETHIOPIA
BRUNEI
Juba
Kuala Lumpur
Male
MALAYSIA
PALAU
Tarawa
Yaounde
UGANDA
KENYA
Mogadishu
MALDIVES
Singapore
Kampala
Borneo
DEM.REP. OF THE CONGO
CONGO
RWANDA
Nairobi
INDONESIA
PAPUA NEW GUINEA
Yaren
NAURU
BURUNDI
Sumatra
Kinshasa
TANZANIA
Victoria
Jakarta
Java Sea
Dodoma
Dar Es Salaam
SEYCHELLES
Java
Dili
EAST TIMOR
Port Moresby
Honiara
Funafuti
TUVALU
ANGOLA
COMOROS
MALAWI
SOLOMON ISLANDS
ZAMBIA
Lilongwe
Lusaka
MADAGASCAR
Coral Sea
VANUATU
Port Vila
Suva
FIJI
Harare
ZIMBABWE
MAURITIUS
Antananarivo
Port Louis
NAMIBIA
BOTSWANA
Windhoek
MOZAMBIQUE
Gaborone
Pretoria
Maputo
AUSTRALIA
Great Barrier Reef
Johannesburg
SWAZILAND
INDIAN OCEAN
Brisbane
Great Victoria Desert
Great Dividing Range
LESOTHO
Durban
SOUTH AFRICA
Perth
Cape Town
Sydney
Adelaide
Canberra
Auckland
Melbourne
NEW ZEALAND
Tasman Sea
Wellington
SOUTHERN OCEAN
C T I C A

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE