For Immediate Release:
February 10, 2020

Contact: (301) 243-0408
DNI_NCSC_OUTREACH@dni.gov

NCSC Unveils the National Counterintelligence Strategy of the U.S. 2020-2022

The National Counterintelligence and Security Center (NCSC) today unveiled the *National Counterintelligence Strategy of the United States of America 2020-2022,* outlining a new approach to counterintelligence to address threats that have evolved significantly since the last strategy in 2016.

"Today's strategy represents a paradigm shift in addressing foreign intelligence threats as a nation. While past counterintelligence strategies categorized the threat by our top foreign nation-state adversaries, this one focuses on five key areas where foreign intelligence entities are hitting us hardest and where we need to devote greater attention – critical infrastructure, key U.S. supply chains, the U.S. economy, American democratic institutions, and cyber and technical operations," said NCSC Director William Evanina.

"With the private sector and democratic institutions increasingly under attack, this is no longer a problem the U.S. Government can address alone. It requires a whole-of-society response involving the private sector, an informed American public, as well as our allies," Director Evanina added.

According to the strategy, which was signed by President Trump on January 7, 2020 and is available at www.ncsc.gov, three principal trends characterize today's counterintelligence threat landscape.

- **The number of threat actors targeting the U.S. is growing**, ranging from state actors like Russia, China, Iran, Cuba, and North Korea; to non-state actors like Lebanese Hizballah, ISIS and al-Qa'ida; to hacktivists, leaktivists and those with no formal ties to foreign intelligence services.

- **These threat actors have increasingly sophisticated intelligence capabilities and technologies at their disposal**, including advanced cyber tools, biometric devices, high-resolution imagery, enhanced technical surveillance equipment, advanced encryption and big data analytics.

- **Threat actors are using these enhanced capabilities against an expanded set of targets and vulnerabilities**. While foreign intelligence entities are targeting most federal agencies in the U.S. -- including those without a national security mission -- they are also targeting a broad array of private sector and academic entities and seeking to influence U.S. public opinion.

To anticipate and deter these threats, the U.S. Government will continue to address its fundamental counterintelligence missions. These include countering foreign intelligence activities in the U.S., mitigating insider threats, protecting U.S. sensitive and classified information as well as sensitive facilities from technical penetrations or espionage, and countering assassination attempts by foreign intelligence services.

However, the 2020-2022 strategy goes beyond these traditional government-centric missions to focus on critical infrastructure, key U.S. supply chains, the U.S. economy, American democratic institutions, and cyber and technical operations. It is in these areas where the strategy says investment in

capabilities and resources are required to strengthen national security. The strategy's five strategic objectives, all equally important, are:

- **Protect the nation's critical 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 our critical infrastructure, likely in an effort to influence or coerce U.S. decision makers in a time of crisis by holding critical infrastructure at risk of disruption.

- **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 represents a growing threat. Adversaries are attempting to access our nation's supply chains at multiple points by inserting malware into important information technology networks and communications systems.

- **Counter the exploitation of the U.S. economy** to protect our competitive advantage in world markets and our economic prosperity and security. Because the U.S. is a global leader in high-technology research and innovation, America is a tremendous target for the theft or acquisition of critical technology and intellectual property, costing the U.S. hundreds of billions of dollars annually and reducing U.S. economic and military competitive advantage globally.

- **Defend American democracy against foreign influence threats** to protect America's democratic institutions and processes and preserve our culture of openness. Foreign intelligence entities are conducting influence campaigns to undermine confidence in our democratic institutions and processes, sow divisions in our society, exert leverage over America and weaken our alliances.

- **Counter foreign intelligence cyber and technical operations** that are harmful to U.S. interests. This critical objective applies to all the other objectives of the strategy. The development of next generation technologies such as the Internet of Things, 5G technology, quantum computing, and artificial intelligence will present new opportunities for foreign adversaries to collect intelligence and conduct cyber operations against the United States.

The strategy recognizes the U.S. Government cannot address these challenges alone and calls for a whole-of-society approach that fully integrates the assistance of the private sector, an informed public, as well as foreign allies. Sound counterintelligence and security procedures must become part of everyday American business practices. Implementing the strategy will require partnerships, information sharing, and innovation across public and private sectors.

The strategy also makes clear that the U.S. must leverage all instruments of American power, including offensive and defensive counterintelligence measures, to meet these increasing challenges. Federal departments and agencies must align their plans to the five key objectives in the strategy, identify resource requirements and evaluate their performance against the strategy's five objectives.

NCSC is a center within the Office of the Director of National Intelligence. NCSC is the nation's premier source for advancing counterintelligence and security expertise and a trusted mission partner in protecting America against foreign and other adversarial threats.

# # #