For Immediate Release:
August 1, 2024

Contact: (301) 243-0403
DNI_NCSC_OUTREACH@dni.gov

NCSC Unveils the New National Counterintelligence Strategy

WASHINGTON, DC -- The National Counterintelligence and Security Center (NCSC) today unveiled the new *National Counterintelligence Strategy*, which can be accessed at www.ncsc.gov.

"Today's strategy is designed to drive integration, action, and resources across the counterintelligence (CI) community to outmaneuver and constrain foreign intelligence entities (FIEs), protect America's strategic advantages, and invest in the future to meet tomorrow's threats," said NCSC Director Michael Casey. "Developed with our partners across the U.S. government, the strategy provides a comprehensive vision and direction for the CI community to address increasingly complex foreign intelligence threats."

Signed by President Biden today, the strategy updates CI priorities based on current and anticipated threats and communicates these priorities to the CI community, federal, state, and local partners, as well as Congress, industry, academia, foreign partners, and the public. The strategy provides a framework for strategic planning, resourcing, and evaluation. It also aligns CI community efforts with the *U.S. National Security Strategy* and other national strategies to drive progress in key CI mission areas.

Three key pillars govern the strategy: 1) outmaneuver and constrain FIEs; 2) protect U.S. strategic advantages; and 3) invest in the future. These pillars are supported by nine goals that provide strategic direction to the CI community to:

- **Detect, understand, and anticipate foreign intelligence threats**, identify opportunities for action, and provide decision advantage.

- **Counter, degrade, and deter foreign intelligence activities and capabilities** through coordinated offensive and defensive measures.

- **Combat foreign intelligence cyber activities** through proactive, integrated operations.

- **Protect individuals against foreign intelligence targeting and collection**, including Americans and others affiliated with the U.S. government at home and abroad and other protected individuals in the United States who may be of high interest to FIEs.

- **Protect democracy from FIE malign influence** efforts to safeguard the integrity of and public trust in our democratic institutions and processes.

- **Protect critical technology and U.S. economic security** to safeguard our national security and competitive advantage.

- **Protect the nation's critical infrastructure** by increasing understanding and awareness of FIE capabilities and threats, enhancing resilience, denying adversary access, and deterring FIE threats.

- **Reduce risks to key U.S. supply chains** from FIE exploitation and compromise.

- **Build CI capabilities, partnerships, and resilience** to achieve enduring superiority over our FIE adversaries.

Each of these nine strategic goals are supported by a number of specific objectives for the CI community to accomplish. Countering this wide array of evolving threats, however, 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 the public. This unclassified strategy provides the foundation to effectively drive an integrated and coordinated response to our most significant FIE threats.

This strategy will be followed by a classified implementation plan to direct more specific actions and initiatives for the CI community. The implementation plan will be focused on engaging partners, sharing information, identifying and mitigating vulnerabilities, strengthening our defenses, building capabilities and resilience, and working together to protect our people, institutions, and strategic advantages.

NCSC leads and supports the U.S. government's CI and security activities critical to protecting our nation; provides CI outreach to U.S. private sector entities at risk of foreign intelligence penetration; and coordinates the dissemination of public warning regarding intelligence threats to the U.S.

# # #