For Immediate Release:
3 September 2019

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

NCSC and the National Insider Threat Task Force Launch
"National Insider Threat Awareness Month" in September 2019

The National Counterintelligence and Security Center (NCSC) and the National Insider Threat Task Force (NITTF) are today partnering with federal agencies across the government to launch "National Insider Threat Awareness Month" during September 2019.

Throughout September, the Office of the Director of National Intelligence, the Department of Defense, the FBI, the Department of Homeland Security, the Department of State and other federal agencies will be holding events to emphasize the importance of safeguarding our nation from insider threats and to share best practices for mitigating those risks.

The goal of this campaign is to educate federal employees, private sector stakeholders and other audiences about the serious risks posed by insider threats, while encouraging employees to recognize and report anomalous activities so early intervention can occur, leading to positive outcomes for at-risk individuals and reduced risks to organizations.

"All organizations are vulnerable to insider threats from employees who may use their authorized access to facilities, personnel or information to harm their organizations -- intentionally or unintentionally," said NCSC Director William Evanina. "The harm can range from negligence, such as failing to secure data or clicking on a spear-phishing link, to malicious activities like theft, sabotage, espionage, unauthorized disclosure of classified information or even violence."

Director Evanina added, "Most insider threats display concerning behaviors before engaging in negative events. Our objective is to help government and corporate organizations get ahead of the problem by bolstering their insider threat programs so they can detect, engage and assist at-risk employees before they go down the wrong path."

Recent reports underscore the impact of insider threats to both government and businesses.

- **Violence** -- Coast Guard Lt. Christopher Hasson was arrested in February on weapons and drug charges after the FBI found 15 firearms and more than 1,000 rounds of ammunition in his residence. In court documents, prosecutors alleged Hasson is "a domestic terrorist, bent on committing acts dangerous to human life that are intended to affect governmental conduct." In May, Virginia Beach city employee DeWayne Craddock opened fire inside a Virginia Beach municipal building, killing 12 people before

police fatally shot him. In February, Gary Martin killed five co-workers at a manufacturing plant in Aurora, Ill., after being fired at a meeting.

- **Betrayal** -- In July, former State Department employee Candace Claiborne was sentenced to prison for lying about receiving tens of thousands of dollars in gifts from Chinese intelligence agents in exchange for providing them with internal State Department documents. In February, former U.S. service member and counterintelligence agent Monica Witt was indicted for conspiracy to deliver and delivering national defense information to the Iranian government. As part of this effort, she allegedly helped Iranian hackers target her former U.S. Intelligence Community co-workers and colleagues with cyberattacks.

- **Cyber Incidents** -- An Office of Management and Budget report released in August found that more than half (16,604) of the 31,107 reported cybersecurity incidents suffered by the federal government in Fiscal Year 2018 resulted from email/phishing attacks that federal employees fell for, or from improper use of computer systems by employees with authorized access. Meanwhile, an indictment unsealed in August detailed how a Pakistani national and his co-conspirators paid AT&T insiders more than $1 million in bribes to unlock more than 2 million cell phones by installing malware and unauthorized hardware on AT&T's computer systems.

- **Unauthorized disclosure / retention of classified information** -- In July, former National Security Agency (NSA) contractor Harold Martin was sentenced to prison for stealing and retaining classified information at his home. In May, former National Geospatial-Intelligence Agency contractor Daniel Hale was arrested for allegedly disclosing classified information to a reporter. Last October, former FBI agent Terry Albury was sentenced to prison for disclosing classified information to a reporter, while last August, former NSA contractor Reality Winner was sentenced to prison for providing classified information to a news outlet.

- **Theft of intellectual property** -- Last week, former Google executive Anthony Levandowski was indicted on charges of theft of trade secrets on autonomous vehicles from Google. In April, an indictment was unsealed charging former General Electric (GE) employee Xiaoqing Zheng with conspiring to steal GE turbine technologies for China while employed by GE. In December, an individual was charged with theft of trade secrets related to a product worth more than $1 billion from his U.S.-based petroleum company employer. An indictment unsealed last October detailed how Chinese intelligence officers recruited an aerospace company employee to install malware on a company laptop to facilitate cyber intrusions and theft of trade secrets.

Pursuant to a 2011 Executive Order (13587), all federal agencies with access to classified information are required to have their own insider threat detection and prevention programs. The Executive Order also directed the creation of the National Insider Threat Task Force (NITTF) under the leadership of the Attorney General and the Director of National Intelligence. NITTF is co-directed by the FBI and NCSC.

Since its inception, the NITTF has been working to assist federal agencies build programs at their agencies that deter, detect and mitigate insider threats, taking into account the distinct needs, missions and systems of each individual agency. NITTF assistance has included:

- Providing training to thousands of insider threat practitioners in government and businesses
- Publishing national policy, minimum standards and a maturity framework for federal insider threat programs
- Conducting independent assessments of federal insider threat programs
- Providing insider threat trend analysis, technical assistance, guidance and best practices
- Engaging internal and external partners to help insider threat programs develop

For more insider threat resources, visit the NITTF website. It is important to note that insider threat programs across the U.S. government target anomalous activities, not individuals. Each agencies' insider threat program is coordinated with their respective legal counsel, civil liberties, and privacy officials to guarantee civil liberties, privacy, and whistleblower protections.

# # #