NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

For Immediate Release:
3 September 2024

Contact: NCSC_Outreach@odni.gov

NCSC and Partners Focus on "Deter, Detect, Mitigate" During National Insider Threat Awareness Month 2024

WASHINGTON, D.C. -- The National Counterintelligence and Security Center (NCSC), the National Insider Threat Task Force (NITTF), the Office of the Under Secretary of Defense Intelligence and Security (OUSD (I&S), and the Defense Counterintelligence and Security Agency (DCSA) launched National Insider Threat Awareness Month (NITAM) 2024.

NITAM is an annual campaign during September to educate government and industry about the risks posed by insider threats and the role insider threat programs play in deterring, detecting, and mitigating such threats. Federal insider threat programs are comprised of multi-disciplinary teams that address insider threats while protecting workforce privacy and civil liberties. For additional information about the NITAM 2024 campaign and resources available to organizations, visit the NITAM 2024 website.

All organizations are vulnerable to insider threats. An insider threat is anyone with authorized access who uses that access to wittingly or unwittingly harm an organization or its resources. The damage resulting from insider threats can range from espionage, cyber intrusions, and unauthorized disclosures, to theft, sabotage, and workplace violence. Most insider threats exhibit concerning behavior prior to committing negative workplace events. If identified early, many insider threats can be mitigated before harm occurs.

Deter. Detect. Mitigate.

"Every year, the insider threat community rallies around a common theme to help raise awareness of insider threats and share mitigation best practices," said NCSC Director Michael Casey. "The theme of this year's campaign is Deter. Detect. Mitigate. Organizations across government and industry continue to be victimized by insider threats – with serious economic and national security implications -- so it's critical they take the time to engage their workforces on effective ways to deter, detect, and mitigate this persistent threat."

Everyone has a role in deterring, detecting, and mitigating insider threats -- from organizations writ large, to security personnel, supervisors, and frontline employees. Organizations can implement principles of organizational justice to deter insider threats by creating a positive workplace culture that reduces the likelihood of insiders becoming threats. Security or cybersecurity personnel can leverage reporting from user activity monitoring to detect potential concerns and risks. Supervisors can incorporate positive deterrence practices into

their management style to deter and mitigate potential risks. Employees can learn to recognize concerning situations in the workplace as well as those that target the workplace, such as attempts to elicit information about their organization through phishing, vishing, and smishing.

Throughout September, various agencies across the U.S. government plan to hold events to reinforce the value of insider threat programs, highlight the risks posed by insider threats, and share best practices for mitigation.

Recent examples underscore the damage that can be caused by insider threats:

- In August 2024, a U.S. Army intelligence analyst pleaded guilty to conspiracy to obtain and disclose national defense information, exporting technical data related to defense articles without a license, conspiracy to export defense articles without a license, and bribery of a public official.

- In May 2024, a former Central Intelligence Agency (CIA) officer, pleaded guilty to conspiring to gather and deliver national defense information to the People's Republic of China (PRC).

- In April 2024, a former National Security Agency (NSA) employee was sentenced to 262 months in prison for attempted espionage in connection with his efforts to transmit classified national defense information to an agent of the Russian Federation.

- In January 2024, three former Department of Homeland Security (DHS) employees were sentenced for a conspiracy to steal proprietary software and sensitive law-enforcement databases from the U.S. government for use in a commercial venture.

Since its inception more than a decade ago, the NITTF, which is housed at NCSC, has worked with federal agencies to help them build programs that deter, detect, and mitigate insider threats. The October 2011 Executive Order 13587 required all federal agencies with access to classified information to develop their own insider threat programs while also directing the creation of the NITTF under the leadership of the Attorney General and the Director of National Intelligence.

# # #