For Immediate Release:
1 September 2022

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

NCSC and Federal Partners Focus on Countering Risk in Digital Spaces during National Insider Threat Awareness Month 2022

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, the Defense Counterintelligence and Security Agency, and the Department of Homeland Security today launched the fourth-annual "National Insider Threat Awareness Month" (NITAM).

NITAM is an annual, month-long campaign during September to educate government and industry about the risks posed by insider threats and the role of insider threat programs. The campaign seeks to encourage government and private industry employees to recognize and report behaviors of concern, leading to early intervention and positive outcomes for at-risk individuals and reduced risks to organizations. To learn more about the campaign and resources available to organizations, visit the NITAM 2022 website.

An insider threat is anyone with authorized access who wittingly or unwittingly harms an organization through their access. Most insider threats exhibit risky behavior prior to committing negative workplace events. If identified early, many insider threats can be mitigated before harm occurs. Federal insider threat programs are composed of multi-disciplinary teams that address insider threats while protecting privacy and civil liberties of the workforce, maximizing organizational trust, and ensuring positive work cultures that foster diversity and inclusion.

Fostering Critical Thinking in Digital Spaces

This year's NITAM campaign focuses on the importance of critical thinking to help workforces guard against risk in digital spaces, which can facilitate insider threat activity. Such risk includes social engineering efforts; online solicitation by foreign or domestic threats; misinformation, disinformation, and mal-information; as well as malicious cyber tactics like phishing, smishing, and vishing.

With virtual work environments becoming more prevalent, malicious actors have more opportunities to target those in our workforces through exploitation of the digital information landscape. Government and industry employees are often susceptible to malicious digital approaches, posing enhanced risk to themselves and their organizations. The ability to spot and respond to manipulative information begins with critical thinking skills, which are essential to reducing vulnerability to these risks.

"Our trusted workforces (our insiders) are some of the most valuable assets in our nation, but they face an increasingly challenging risk environment," said NCSC Deputy Director Michael Orlando. "It is imperative that we arm our trusted insiders with the resources and skills to counter increasingly sophisticated efforts to exploit our personnel, information, and resources."

“Increasing the workforce's awareness of manipulated information and attempts at online social engineering is critical to ensuring our trusted workforce remains resilient and vigilant against these threats,” said Ronald Moultrie, Under Secretary of Defense for Intelligence and Security.

Today, insider threat practitioners from across the U.S. Government and industry will participate in the 2022 Insider Threat Virtual Conference, hosted by the Department of Defense, to kick off the NITAM 2022 campaign. The 2022 Insider Threat Virtual Conference features senior level speakers and panelists who will present on critical thinking for the workforce, social engineering threats, an insider threat case study, and resources for workforce resiliency to counter insider risk.

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

- In August 2022, a federal jury in California convicted Ahmad Abouammo, a former manager at Twitter, of acting as an unregistered agent of Saudi Arabia and other violations. Abouammo had used his position at Twitter to access, monitor, and convey the private information of Twitter users, including critics of the Saudi regime, to officials of the Kingdom of Saudi Arabia and the Saudi Royal family in exchange for bribes worth hundreds of thousands of dollars.

- In July 2022, a federal jury in New York convicted former CIA programmer Joshua Schulte of violations stemming from his theft and illegal dissemination of highly classified information. Harboring resentment toward CIA, the programmer had used his access at CIA to some of the country’s most valuable intelligence-gathering cyber tools to covertly collect these materials and provide them to WikiLeaks, making them known to the public and to U.S. adversaries.

- In June 2022, civilian defense contractor Shapour Moinian pleaded guilty in California to federal charges, admitting that he acted as an unregistered agent of China and accepted money from Chinese government representatives to provide them aviation-related information from his U.S. intelligence community and defense contractor employers. An individual in China posing online as a job recruiter had contacted Moinian offering him a consulting opportunity. Moinian later traveled to China and other locations where he supplied US aviation information to individuals he knew were employed by or directed by the Chinese government in exchange for money.

It has been more than 10 years since Executive Order 13587 required all federal agencies with access to classified information to have their own insider threat prevention programs and directed the creation of the NITTF under the leadership of the Attorney General and the Director of National Intelligence.

NITTF is currently housed at NCSC. Since its inception, the NITTF has worked with federal agencies to build programs that deter, detect, and mitigate insider threats. NITTF and NCSC coordinate insider threat training and awareness; liaison and assistance; governance and advocacy; and research and analysis for stakeholders in the public and private sector to reduce the risk of insider threats to public health and safety, economic security, and national security.

# # #