THEME: CRITICAL THINKING IN DIGITAL SPACES

CDSE and OUSD(I&S)

2022 National Insider Threat Awareness Month Communications Plan

Introduction:

This communications plan supports the roll-out of the fourth annual National Insider Threat Awareness Month (NITAM) campaign and aims to build off previous successes and expand the impact and audience of the campaign. NITAM highlights the importance of insider threat awareness in preserving our personal safety, strong economy, and national security and challenges all Americans to help protect, preserve, and strengthen our public and private organizations. NITAM also helps to educate government personnel and outside audiences on how to recognize and report potential risk indicators.

The proper introduction of NITAM to the audience is critical. National Insider Threat Task Force (NITTF), DOD, Defense Counterintelligence and Security Agency (DCSA), and other stakeholder organizations have made every effort to ensure adherence to ethical, legal, and regulatory standards in the development and implementation of this program and those standards will continue to be upheld by all insider threat (InT) programs. This fact must be appropriately communicated to employees at the onset of the rollout.

Background:

Insider threats are individuals with authorized access who wittingly or unwittingly use that access to harm their organization and its resources. Insiders can include employees, vendors, partners, suppliers, and others. Insider incidents impact both public and private institutions, causing damage to national security, loss of life, the loss or compromise of classified or sensitive information, and billions of dollars annually in lost revenue related to trade secret theft, fraud, sabotage, damage to an organization's reputation, acts of workplace violence, and more. Most insider threats exhibit known or knowable concerning behavior prior to committing malicious acts. If identified early, many risks can be mitigated before harm occurs.

In October 2011, the president issued Executive Order (E.O.) 13587 directing federal departments and agencies with access to classified information to establish insider threat detection and prevention programs. In November 2012, the president issued the National Insider Threat Policy and the Minimum Standards. Next, there was a specific policy for DOD components, DODD 5205.16 in September 2014, and industry under the National Industrial Security Program (NISP) in May 2016. More recently, a 2017 memo from the Deputy Secretary of Defense recommended a new strategy to manage violent behavior and similar threats, which led to the creation of the prevention assistance response (PAR) capabilities requirements. Taken together, these policy and memoranda proactively and comprehensively identify and mitigate risks associated with insider threats.

Communications Objectives:

- Increase employee awareness across the general workforce (DOD, federal agencies, industry, and secondary audiences) of the possible risks posed by trusted insiders

- Increase employee awareness regarding the nation's vulnerability to insider threats and emphasize the individual's responsibility to recognize and report concerning behavior

- Introduce insider threat programs to strategies designed to deter, detect, and mitigate risks

- Promote the goal of early intervention and ensure communications maximize transparency and minimize misconceptions associated with insider threat programs
- Introduce methods to dispel efforts by adversaries to radicalize or malign the workforce
- Increase employee awareness of digital space as a threat environment; and risks posed to trusted insiders navigating social media and online new outlets.

Intended Outcomes:

The NITAM communications goals will be achieved through the following objectives:

OUTCOME 1: Increased partnership, research, and engagement on initiatives related to bolstering critical thinking among the DoD workforce

OUTCOME 2: Increased awareness of risk factors by general workforce to prevent insider threat incidents down the road

OUTCOME 3: Enhanced knowledge of networks of prevention and assistance resources for the workforce

OUTCOME 4: Expanded network of prevention and assistance resources for the workforce to include available training and education

Communications Stakeholders/Partners:

The following stakeholder and partner organizations have a critical stake in NITAM's success. Together, these stakeholders blend a tactical, on-the-ground perspective with behavioral and social science research to elevate the strategic messaging, impact, and scope of the campaign.

DOD Stakeholders	USG Stakeholders	Partners in Academia
OUSD(I&S)	NITTF	US CERT/Carnegie Mellon
DCSA – CDSE, CTP, Vetting and Background Investigation	DHS	West Point
DITMAC	FBI	ARLIS at University of Maryland
DOD EPMO	Executive Branch ITPs	
DOD PERSEREC	State Department	
DOD Component ITPs		

Communications Audiences:

- Primary: InT program personnel and leadership at DOD components, federal agencies, and industry under the National Industrial Security Program or at Critical Infrastructure Key Resource organizations

- Secondary: General workforce of DOD components, federal agencies, and industry under the NISP or at critical infrastructure key resource organizations, academia, mental health professionals, HR professionals, general public

Key Messages:

The theme for 2022 is **Critical Thinking in Digital Spaces; sub-themes include Digital Media Literacy, Online Manipulation of Perceptions, and Cognitive Bias. Campaign Message: "Disinformation Stops With You".**

- Increase awareness and understanding of why critical thinking is key to preventing unwitting and witting insider threats and protecting national security. Critical thinking will help individuals become less susceptible to various types of risks, to include social engineering, solicitation by adversaries, (foreign and domestic) and information designed to malign.

- Individuals/organizations achieve a greater understanding of how virtual platforms have been utilized by malicious actors and how to spot efforts to intentionally manipulate perceptions.

- COVID, isolation, and working from home has made it more difficult to discern between true coworkers and phishing attempts for proprietary or sensitive information. It has also lead to more interactions on social media which makes individuals more vulnerable to deception.

Perennial themes include Resilience, Vigilance, Safety, Security, the Counterintelligence Threat, Recognizing and Reporting indicators, Proactive Nature of Insider Threat Programs, and Respect for Privacy and Civil Liberties.

- Insider incidents impact public and private organizations by causing damage to national security, loss of life, the loss or compromise of classified information, and billions of dollars annually in lost revenue related to trade secret theft, fraud, sabotage, damage to an organization's reputation, acts of workplace violence, and more.

- Compromises by insiders have made America less safe by allowing our adversaries to access classified information, change tactics and avoid detection, and learn where we are most vulnerable.

- Most insider threats display concerning behaviors or risk indicators prior to engaging in malicious acts.

- Insider threat programs are designed to detect, prevent, and mitigate risks associated with malicious or unwitting insiders while protecting privacy and civil liberties.

- Reporting concerning behaviors and risk indicators allows insider threat programs to take proactive measures that will hopefully lead to positive outcomes for individuals and mitigate risk for organizations.

Platforms:

- Websites
  - Designated Insider Threat Awareness Month website
    - CDSE NITAM Awareness: https://securityawareness.usalearning.gov/cdse/itawareness/index.html
  - Stakeholder Websites:
    - ODNI NITAM: https://www.dni.gov/index.php/ncsc-features/2834-september-2021-is-national-insider-threat-awareness-month
  - Partner Websites

- Banners/Features/Dedicated Real Estate

- Social Media
  - Twitter: @InT_Aware
  - Facebook: CDSE Insider Threat Awareness, CDSE, DCSA
  - Stakeholder accounts: @TheCDSE, @DCSAgov, @ODNIgov @NCSCgov @DHSgov

- Insider Threat Sentry Mobile Application:
  - Push notifications, event calendar, content distribution

- Leadership media engagement:
  - Press/Podcasts/Video

- Print/Products

Roles and Responsibilities:

CDSE

- Co-host OUSD(I&S)/DOD Insider Threat event September 1
- Draft and coordinate communications plan
- Use social media handles for Insider Threat Awareness Month (@InT_Aware, CDSE Insider Threat Awareness)
- Support logistics for OUSD(I&S)/DOD Insider Threat event September 1
- Launch NITAM 2022 website
- Manage and develop products for InT Sentry app
- Coordinate with DCSA Communications and Public Affairs Office (PAO) to review and approve materials

- Develop press kit or articles with messaging for components and stakeholders to use.
- Coordinate and attend stakeholder meetings
- Coordinate with DCSA social media platforms to post messaging and repost or otherwise engage with approved messaging from additional partners and stakeholders.
- Encourage DCSA leadership to engage with traditional media and press for interviews, articles, op/eds
- Coordinate survey or other evaluation techniques
- Draft after-action report

OUSD(I&S)

- Draft and coordinate OUSD(I&S) letter
- Co-host OUSD(I&S)/DOD Insider Threat event September 1
- Coordinate with OUSD(I&S) and DOD leadership on DOD Enterprise Leadership Statement and potential media appearances and/or additional content
- Develop thematic graphics for Pentagon-specific audiences
- Coordinate with DOD web and media platforms to post messaging and repost or otherwise engage with approved messaging from additional partners and stakeholders
- Coordinate additional activities including literature distribution within the Pentagon in September
- Coordinate speakers/agendas
- Attend stakeholder meetings for DOD components
- Support survey or other evaluation techniques

DOD Liaison to NITTF

- Contribute to development of messaging and content
- Promote NITAM to DOD components
- Attend stakeholder meetings
- Support survey or other evaluation techniques

DITMAC/DOD Insider Threat EPMO

- Contribute to development of messaging and content
- Promote NITAM to DOD Components
- Attend stakeholder meetings
- Support survey or other evaluation techniques

NITTF

- Draft and Coordinate National Counterintelligence and Security Center (NCSC) Director letter
- Coordinate with NCSC and DNI leadership for potential media appearances and/or content
- Coordinate with NCSC and DNI social media platforms to post messaging and repost or otherwise engage with approved messaging from additional partners and stakeholders
- Promote NITAM to federal agencies
- Host meeting with identified partners in federal agency insider threat programs

- Support survey or other evaluation techniques

DCSA CTP Policy, Vetting and BI

- Contribute to development of messaging and content
- Promote NITAM to industry
- Attend stakeholder meetings
- Host partner meeting for industry
- Support survey or other evaluation techniques

DHS

- Contribute to development of messaging and content
- Promote NITAM to critical infrastructure sectors
- Attend stakeholder meetings
- Host partner meeting for Critical Manufacturing and/or additional sector working groups as applicable
- Coordinate with DHS social media platforms to post messaging and repost or otherwise engage with approved messaging from additional partners and stakeholders
- Support survey or other evaluation techniques

DOD Components

- Develop additional or custom material for their organizations to include poster or ad contests, fun runs, insider threat "days," and other items outlined in the communications packet
- Encourage leadership to engage with traditional media and press for interviews, articles, op/eds Repost/retweet content from official Insider Threat social media channels

PERSEREC

- Contribute to development of messaging and content
- Promote NITAM to academia
- Attend stakeholder meetings
- Coordinate with DOD social media platforms to post messaging and repost or otherwise engage with approved messaging from additional partners and stakeholders
- Launch Social and Behavioral Science Summit
- Support survey or other evaluation techniques

FBI/State Department

- Contribute to development of messaging and content
- Promote NITAM to workforce, including personnel OCONUS
- Coordinate with respective social media platforms to post messaging and repost or otherwise engage with approved messaging from additional partners and stakeholders

Evaluation:

OBJECTIVE 1: Use messaging vehicles to track impressions, mouse clicks, downloads, etc. By tallying the amount of internet traffic to this content, we can identify a general figure for overall engagement.

OBJECTIVE 2: Follow NITAM events with survey to insider threat program managers to gauge interest, engagement, response, and reporting.

OBJECTIVE 3: Quantify engagement with external industry and academia through the number of speakers, percentage of audience attendance/participation from industry/non-USG organizations

Intended Use:

U.S. Department of Defense (DOD), U.S federal agencies, cleared contractors under the National Industrial Security Program (NISP), Human Capital Management Offices, Public Affairs, Security Education, Training, and Awareness (SETA) Managers, and security professional associations can use this communications plan to increase awareness about the 2022 National Insider Threat Awareness Month.