National Insider Threat Awareness Month (NITAM) 2023

Communications Plan & Messaging Packet

DOD Insider Threat Program,
Office of the Under Secretary of Defense for
Intelligence and Security OUSD (I&S)

SLIDES ONLY

NO SCRIPT PROVIDED

Introduction

This communications plan supports the roll-out of the fifth 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.

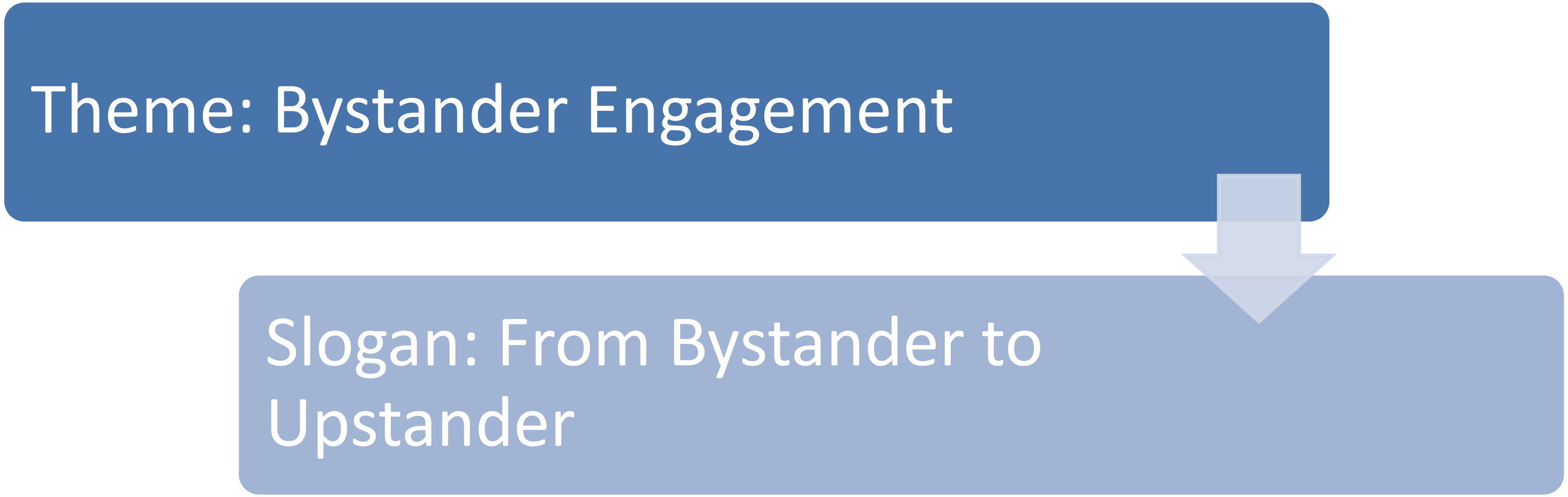
The proper introduction of NITAM to the audience is critical. National Insider Threat Task Force (NITTF), DOD, and other stakeholder organizations have made every effort to ensure adherence to ethical, legal, and regulatory standards in the development and implementation of this program and those standards 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.

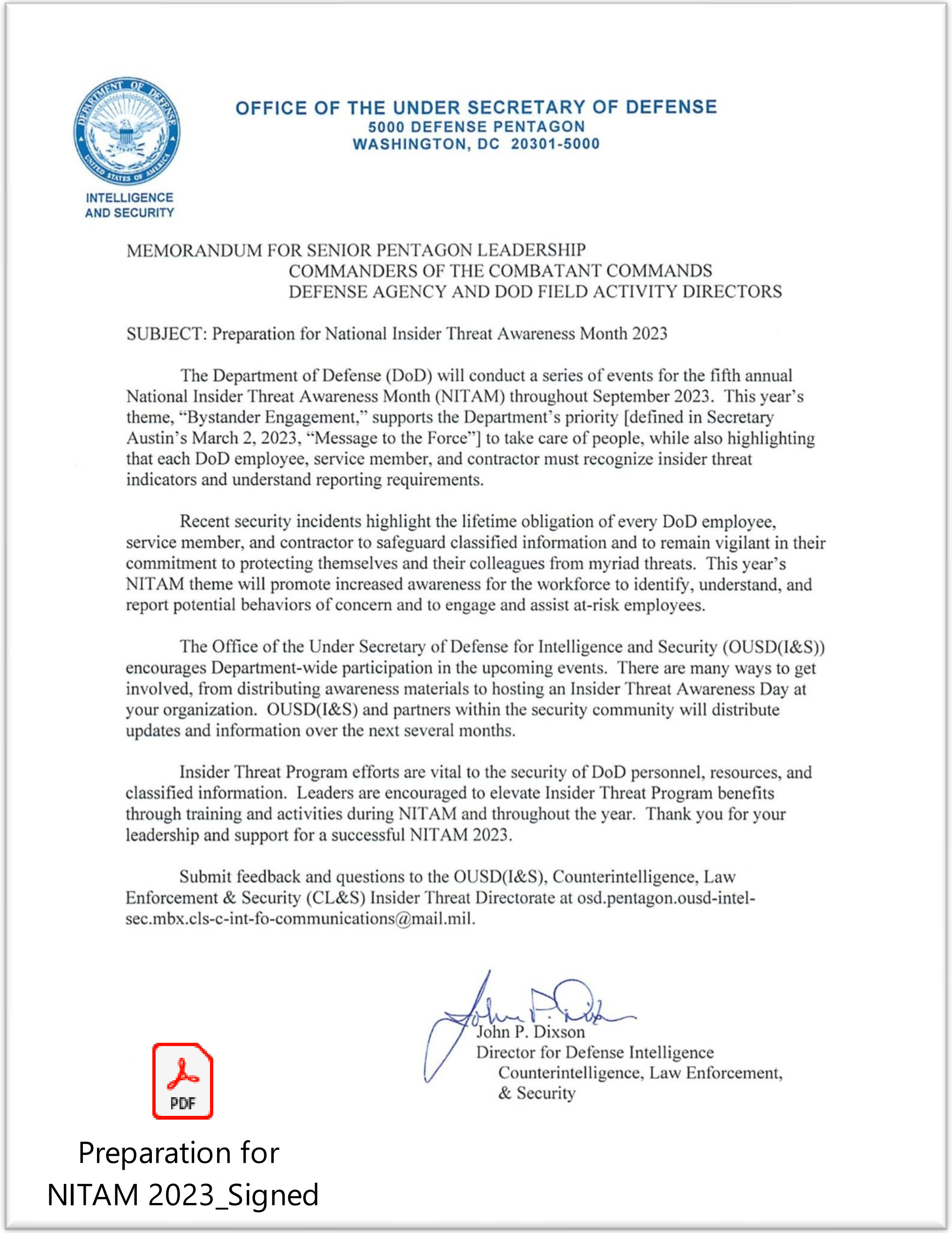
NITAM 2023 Theme



Theme: Bystander Engagement

Slogan: From Bystander to Upstander

Leadership Support Memorandum for NITAM Preparation



OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

INTELLIGENCE
AND SECURITY

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
COMMANDERS OF THE COMBATANT COMMANDS
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Preparation for National Insider Threat Awareness Month 2023

The Department of Defense (DoD) will conduct a series of events for the fifth annual National Insider Threat Awareness Month (NITAM) throughout September 2023. This year's theme, "Bystander Engagement," supports the Department's priority [defined in Secretary Austin's March 2, 2023, "Message to the Force"] to take care of people, while also highlighting that each DoD employee, service member, and contractor must recognize insider threat indicators and understand reporting requirements.

Recent security incidents highlight the lifetime obligation of every DoD employee, service member, and contractor to safeguard classified information and to remain vigilant in their commitment to protecting themselves and their colleagues from myriad threats. This year's NITAM theme will promote increased awareness for the workforce to identify, understand, and report potential behaviors of concern and to engage and assist at-risk employees.

The Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)) encourages Department-wide participation in the upcoming events. There are many ways to get involved, from distributing awareness materials to hosting an Insider Threat Awareness Day at your organization. OUSD(I&S) and partners within the security community will distribute updates and information over the next several months.

Insider Threat Program efforts are vital to the security of DoD personnel, resources, and classified information. Leaders are encouraged to elevate Insider Threat Program benefits through training and activities during NITAM and throughout the year. Thank you for your leadership and support for a successful NITAM 2023.

Submit feedback and questions to the OUSD(I&S), Counterintelligence, Law Enforcement & Security (CL&S) Insider Threat Directorate at osd.pentagon.ousd-intel-sec.mbx.cls-c-int-fo-communications@mail.mil.

John P. Dixson
Director for Defense Intelligence
Counterintelligence, Law Enforcement,
& Security

PDF

Preparation for
NITAM 2023_Signed

Communication Objectives

01

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

02

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

03

Promote the goal of early intervention and ensure communications maximize transparency and minimize misconceptions associated with insider threat programs.

04

Increase employee awareness, methods, and best practices of bystander engagement in identifying and taking action when concerning behaviors are observed.

05

Support Secretary Austin’s “Taking Care of Our People” initiative which includes ‘ensuring accountable leadership’ and ‘build resilience and readiness.’

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 bystander engagement within the general workforce

OUTCOME 2: Increased awareness of risk factors by general workforce to prevent insider threat incidents now and in the future

OUTCOME 3: Enhanced awareness 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 and 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 InTPs	
DOD PERSEREC	State Department	
DOD Component InTPs		

Communication Audiences

Primary: InT program personnel and leadership at DOD components, federal agencies, and industry under the National Industrial Security Program (NISP) 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, and the general public

Key Messaging: Bystander Engagement

The theme for 2023 is **Bystander Engagement; sub-themes include Workplace Toxicity, Information Sharing**

- A **bystander** is someone who witnesses concerning behaviors but may not take action to help mitigate the problem. **Bystander Engagement** is the concept whereby an individual is aware of concerning behaviors, knows how to act on those concerns, and takes appropriate action.
- Increased awareness and understanding bystander engagement will strengthen the workforce and safeguard national security. Understanding bystander engagement will empower individuals to act earlier and more often when identifying concerning behaviors.
- Engaging with distressed individuals can help create positive outcomes for the individuals as well as organizations.
- These themes support Secretary Austin's "Taking Care of Our People" initiative which involves Building Resilience and Readiness as well as Ensuring Accountable Leadership.
- *Department of Defense personnel have privileged access to Classified National Security Information (CNSI), Controlled Unclassified Information (CUI), and unclassified information that has not been approved for public release. It is a violation of law, and of the oath of office to divulge, in any fashion, non-public DoD information to any unauthorized recipient without the required prior approval for access to national security information and specific need to know for CNSI or lawful government purpose for CUI. Willful or negligent disclosure of non-public information outside of those requirements is an unauthorized disclosure (UD) and a serious security incident.*

Key Messaging: Perennial Themes

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.
- Individuals at risk of becoming insider threats, and those who ultimately cause significant harm, often exhibit concerning behaviors. Timely and appropriate sharing of concerning behaviors is crucial for protecting our workforce. Preventing harm due to insider threat is a shared responsibility.

Platforms

Websites

Designated Insider Threat Awareness Month website

- CDSE NITAM Awareness:
    - https://securityawareness.usalearning.gov/cdse/itawareness/index.html

Stakeholder Websites:

- PERSEREC/Threat Lab SBS Summit:
    - https://www.SBSSummit.com
- ODNI NITAM
    - https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf
- USMC NITAM:
    - https://www.information.marines.mil/Units/Insider-Threat/

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

- Posters
- Brochures

Roles & Responsibilities

OUSD(I&S)

- Stand up NITAM WG
- Draft and coordinate OUSD(I&S) endorsement letter
- Support the Threat Lab SBS Summit
  - Participate in speaker selection and logistic planning
  - Promote marketing material and be in attendance
- Support the virtual DCSA Conference for Insider Threat event September 7
  - Participate in Steering Committee
  - Promote marketing material
- Coordinate with OUSD(I&S) and DOD leadership on DOD Enterprise Leadership Statement and potential media appearances and/or additional content
- Coordinate the development thematic graphics for Pentagon-specific audiences
- Coordinate with OSD Public Affairs to support:
  - Social Media messaging
  - Public Service Announcements
- Coordinate Insider Threat Awareness Day, including Information Tables at an Apex
- Attend stakeholder meetings for DOD components
- Create and distribute survey or other evaluation techniques for components engagements

Roles & Responsibilities cont'd

DOD Components

- Participate in OUSD(I&S) supported events, to include the Insider Threat Awareness Day, SBS Summit, and DCSA Virtual Conference for Insider Threat.
- 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

DITMAC

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

CDSE

- Host DCSA Conference for Insider Threat – 7 September 2023 [Registration live on 03 JUL 23: https://www.cdse.edu/Training/Webinars-and-Conferences/]
- Use social media handles for Insider Threat Awareness Month (@TheCDSE)
- Launch NITAM 2023 website [Update live 08 AUG 23: https://securityawareness.usalearning.gov/cdse/nitam/]
- Manage and develop products for NITAM [CDSE-level NITAM PSA, Bystander Engagement and Insider Risk Awareness Video, Posters, Awareness Games, Sentry Executive Magazine – ETA JUL/AUG]
- Co-host Webinar with Navy Insider Threat for 10 Year Anniversary of Navy Yard Shooting – 14 September 2023 [Registration live mid-JUL}
- Coordinate with DCSA Public Affairs to develop outreach kit and press release/article 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
- Draft post-event reports for conference and webinars

Roles & Responsibilities cont'd

PERSEREC/Threat Lab

- 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
- Coordinate and host the Social and Behavioral Science Summit
- Support survey or other evaluation techniques

DHS

- Contribute to development of messaging and content
- Promote NITAM to critical infrastructure sectors
- Attend stakeholder meetings
- 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

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

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

Timeline

Summary Milestones (Projected)	Owner	Due Date (Projected)
Kick-off Meeting	OUSD(I&S)	January 2023
Finalize Communications Plan 1. Message development	OUSE (I&S)	April 2023
Draft Support Memos for Leadership 1. Director of NCSC 2. DOD Leadership (OUSD(I&S))	NCSC OUSD(I&S)	April-May 2023
Develop Content		April-July 2023
Finalize Insider Threat Awareness Day Planning	OUSD(I&S)	June 2023
Launch Campaign including Messaging, New Content Releases, Events, and NITAM Awareness Website	CDSE	June 2023
Finalize Champion Messaging Packet	OUSD(I&S)	July 2023
SBS Summit (in-person)	Threat Lab	August 2023
DCSA Conference for Insider Threat	CDSE	September 2023
Conduct Surveys, Obtain Web and Social Media Metrics	CDSE	October 2023
Complete After-Action Report	OUSD(I&S)	October 2023

Products

CDSE Products	Description

Threat Lab Product	Description
Job Aid	Bystander Engagement Tri-Fold

Graphics

NITAM
National Insider Threat Awareness Month

Click here for all available products & resources!

https://securityawareness.usalearning.gov/cdse/nitam/resources.html

SEPTEMBER IS
NITAM
National Insider Threat Awareness Month
P CONNECT
E DOTS
CHOOSE YOUR OWN
COUNTER-INSIDER THREAT ACTION
THE ANGRY COWORKER
You notice your coworker Alan has been making violent, threatening posts about your agency on social media. You decide to...
INFORMATION SHARING
YOUR ACTIONS CAN MAKE A DIFFERENCE
SUPPORTING through REPORTING
Sharing what you know could help security programs deter, detect, and mitigate the next insider threat.
YOU
CONNECT THE DOTS
NITAM
CDSE

Contacts

This Communications Plan & Messaging Packet was developed by DOD Insider Threat Program, Office of the Under Secretary of Defense for Intelligence and Security OUSD (I&S).

All questions/inquiries should be directed towards:

osd.pentagon.ousd-intel-sec.mbx.dod-counterinsiderthreat@mail.mil