January 2022 Volume 2 | Issue 1

# ENTERPRISE THREAT MITIGATION NEWSLETTER

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

## DoD OPSEC Program: Working to Keep the Department Safe

*Department of Defense, OPSEC Program*

Proper information handling, which is a key part of Operations Security (OPSEC), is crucial to maintaining the Department of Defense's (DoD) advantage over adversaries and strategic competitors who seek to degrade our operations, put the safety of our personnel at risk, and prevent our mission success. The DoD OPSEC program does this by identifying, controlling, and safeguarding critical information and indicators to preserve essential secrecy.


"OPSEC is everyone's responsibility"

In July 2020, the Secretary of Defense launched a campaign to emphasize the importance of OPSEC and reduce unauthorized disclosures (UD) of classified and controlled unclassified information (CUI). The campaign directed several Department-wide actions including training, technology pilots, and the improvement of UD reporting and investigative procedures. In association with this campaign, the Under Secretary of Defense for Intelligence and Security conducted a data call to assess the status of the DoD OPSEC Program. The results revealed many areas where we are excelling at OPSEC, but also revealed areas wherein DoD can improve our OPSEC program through better policy

and training.

DoD fully supports the National Counterintelligence and Security Center's National OPSEC Program efforts to formally recognize January 2022 as the first annual National OPSEC Awareness Month. DoD will use this as an opportunity to reinvigorate our ongoing campaign efforts to promote workforce awareness of proper OPSEC practices, including those related to public disclosure, unauthorized disclosure, and pre-publication review. It is also an opportunity to remind employees about the importance of being deliberate with all classified, controlled unclassified, and pre-decisional policy information and proposals.

OPSEC is everyone's responsibility. Let's all make National OPSEC Awareness Month a resounding success by recommitting to the observance of sound OPSEC practices.

## INSIDE THIS ISSUE

# NTER: A National Framework in Threat Mitigation

*Jennifer Cohen, Department of Homeland Security (DHS)*

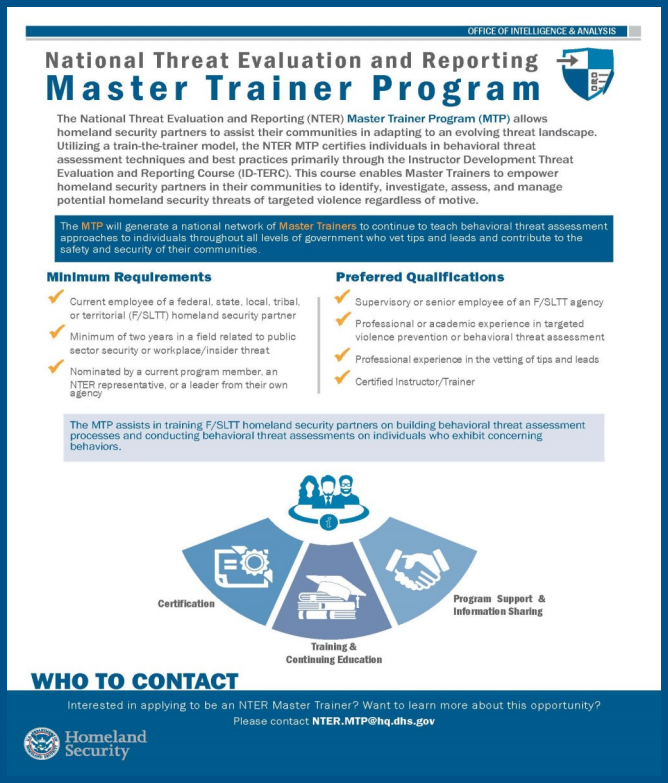
Over the past few decades, the threat landscape has changed in unprecedented ways, opening the aperture beyond ideological threats of violence. Many agencies, organizations, and governing bodies began developing threat mitigation strategies focusing on behavioral aspects to violence prevention using threat assessment methodology. However, today there is a lack of standardization in threat assessment policies, procedures, terminology, and assessment tools across sectors, regions, and jurisdictions. The U.S. Department of Homeland Security, Office of Intelligence and Analysis, National Threat Evaluation and Reporting (NTER) Program, developed a Master Trainer Program (MTP) in an effort to create a national framework and common operating picture in threat assessment and management to assist federal, state, local, tribal, and territorial homeland security partners in preventing targeted violence.

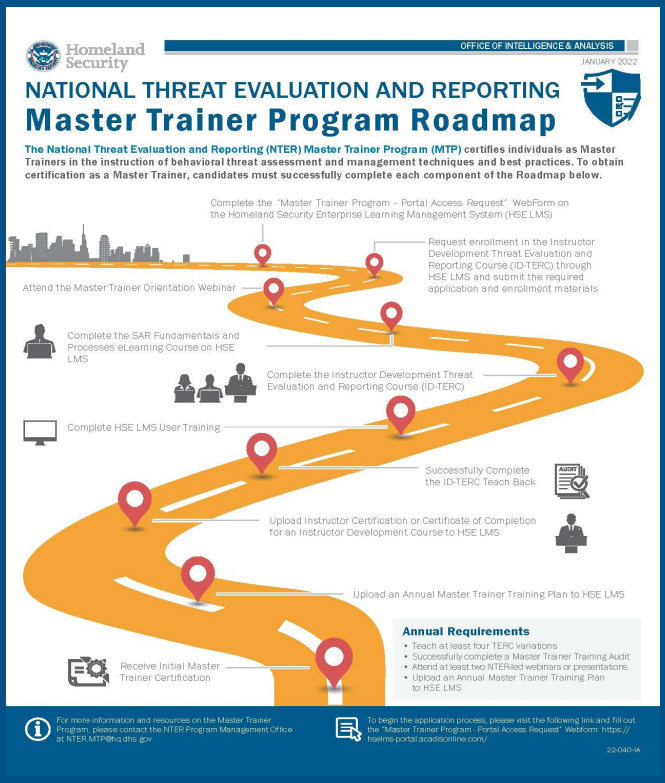
The NTER MTP was built upon the success of the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI), expanding beyond ideological-based violence. NTER leveraged existing threat assessment research, such as foundational documents and studies from the U.S. Secret Service and the Federal Bureau of Investigation, as well as collaborated with elite members of the Association of Threat Assessment Professionals and other distinguished researchers to develop the NTER MTP curriculum.

The MTP utilizes a train-the-trainer model to certify individuals as Master Trainers in behavioral threat assessment techniques and best practices. The cornerstone of the MTP is the Instructor Development Threat Evaluation and Reporting Course (ID-TERC), which empowers homeland partners to identify, investigate, assess, and manage threatening or suspicious behaviors to prevent potential targeted violence incidents. Using NTER-provided resources, certified Master Trainers can teach variations of the ID-TERC curriculum to partners in their agencies and within their areas of responsibility.

To further build a shared understanding of behavioral threat assessment and management, the NTER Program hosts quarterly webinars and disseminates quarterly bulletins on the emerging trends and up-to-date research studies in targeted violence. The NTER Program strives to empower homeland security partners, from all levels of society, in building their capabilities in identifying, evaluating, reporting, and sharing threat information across the nation. You can learn more about NTER at the **National Threat Evaluation and Reporting (NTER) Program | Homeland Security (dhs.gov)**. For questions and comments, and to learn more about how you can get involved, please contact **NTER@hq.dhs.gov**.

## BELOW ARE KEY DETAILS ABOUT THE MTP AND THE CERTIFICATION PROCESS:



# Unauthorized Public Disclosures: The Media and You

You, as a professional with access to classified national security information, are being trusted with the nation's secrets. Secrets, which if disclosed, can have extremely damaging effects to the nation, not to mention the potential for the loss of people's lives. So, it is a very important "trust" you hold and a weighty responsibility to protect those secrets. You accepted that responsibility when you signed your non-disclosure agreement, committing yourself to the safe-handling and protection of the information you would be entrusted with. By virtue of your position and access, there are those out there who would like to know what you know, and they are not always foreign adversaries. The media takes pride in keeping the public informed and journalists are always competing for the next "breaking story". That's their job. And in many cases, that makes you their target.

In a 2017 training article titled, "The steps to finding, developing and vetting news sources", NPR's Chief Diversity Officer lays out, based on interviews with correspondents with years of experience, tips for how successful journalists go about building sources. The portfolios of the three reporters interviewed for the training article included assignments as a national security reporter, a Pentagon reporter, and a Department of Justice reporter. In their own words, here are a few of the techniques, tips, and observations they provided to other journalists in finding and developing sources that we, serving in the national security arena, should be aware of:

*"Go where people are happy." "Dinners, awards ceremonies, receptions, conferences, galas — that's when people are feeling good and less guarded."*

*"Start conversations off by looking for a personal connection."*

*"Learn how they (potential sources) prefer to communicate."*

*"Look for "formers," people who used to hold key positions in the intelligence community but have since retired or changed jobs. They are more helpful when they don't have to worry about being fired for talking..."*

*Reporters "can often get better, more reliable information from the lowest ranking soldiers — preferring privates, not generals." "The guys on the bottom who are seeing what's going on day in and day out, they'll tell you exactly what they think…"*

These are just a few techniques journalists use to get access to sources and information. It is evident the media also uses tradecraft to produce their sources. They are not our adversary, but they have their own agenda, motives, and standards that do not always align with the importance of protecting classified information. They may be in it to advance their career, break a story, or any other number of reasons, and far too often there are those in our profession willing to give up classified information to further their own agenda. As pointed out by one of the journalists interviewed, "…sources have their motives. They might hate their boss, have an axe to grind or think they're a "whistleblower saving the world…" Whatever the motive, these "leaks" to the media are a breach of trust, unlawful, and can be especially damaging to our national security. Remember your oath and commitment to safeguard the information entrusted to you. Be on guard, and don't be the person who jeopardizes our national security, or worse, is responsible for a colleague's death just for the sake of a story!

"[The media] are not our adversary, but they have their own agenda, motives, and standards that do not always align with the importance of protecting classified information."

# An Organization is Only as Good as Its Employees

*Clarissa Gallo, NCSC/ETD Virtual Student Federal Service Intern*

One rule of thumb in business is that employee work performance determines organizational success. But, to a certain degree, the quality of work produced by employees depends on their feelings towards their employer/workplace. A disengaged and dissatisfied workforce risks yielding undesirable consequences, including substandard quality or low productivity, for its organization. To put it briefly: a successful organization needs happy employees.

Understanding what contributes to employee performance is a key to increasing quality and productivity, but that knowledge can also help an organization's leadership understanding maladaptive workplace behaviors and potential insider threat warning signs. When analyzing open-source articles published since 2019 that pertain to workforce engagement, satisfaction, and insider threat, two prevalent themes emerged: (1) leadership and management practices, which then determine (2) the work environment.

Organizations should strive for a positive workplace culture that takes an employee's mental and physical health into account. Leaders should check-in with their employees and ensure proper resources exist to address mental health and employee well-being. In times of high stress, managers can offer help to employees by implementing policies and processes that allow for flexibility, such as giving employees flexibility in their schedules.

Positive workplaces are also engaging environments. Leaders must make themselves visible and available to their employees. Managers should endorse group connection through team-building activities and encourage collaboration among workers. During these activities, proper communication and listening skills should be emphasized so that employees are encouraged to participate.

Insider threat programs can contribute to positive workplace cultures by allowing an organization to identify anomalous behaviors of concern and to intervene before employee well-being is negatively affected. A well-rounded insider threat program, which includes participants from HR, civil liberties, security, etc. can take advantage of all the organization's resources to mitigate potential risks before those risks become a real problem. Organizations should also strive to react to any verified anomalies with an appropriate response level –– in other words, in a manner its workforce perceives as fair and balanced.

Finally, positive workplaces are ethical and fair. Managers must promote equality in the workplace and exercise the company's values. Workers who are treated ethically are more willing to reflect the morals and values of the organization, and mentally and physically healthy workers are less likely to quit their jobs and take days off from work. This reduces costs associated with absenteeism and turnover rates. In addition, safety incidents and insider threat risks further decrease in this environment, especially when employees who collaborate with one another help increase each other's skills and abilities. And when roles

within the organization are clearly defined, everyone knows their responsibilities and will be able to perform their tasks

## CDSE's Insider Threat Vigilance Campaign 2022

*Cashmere He, CDSE, Insider Threat Division*

Throughout 2022, the Center for Development of Security Excellence (CDSE) will be sponsoring an Insider Threat Vigilance Campaign. Regular messaging through communication and awareness materials reinforces annual insider threat awareness training and helps ensure the workforce is prepared to recognize and respond to the insider threat. For the 2022 Insider Threat Vigilance Campaign, CDSE will be promoting a different theme each month and publishing/distributing awareness materials relevant to each theme in unique ways throughout the year. Please see our publication schedule and product links below. *Note, most links will not work until the product has been published at the beginning of each month.*

Use this campaign or consider tailoring it to your organization with resources from our website (**https://www.cdse.edu/Training/Toolkits/Insider-Threat-Toolkit/**).

### INSIDER THREAT VIGILIANCE CAMPAIGN 2022

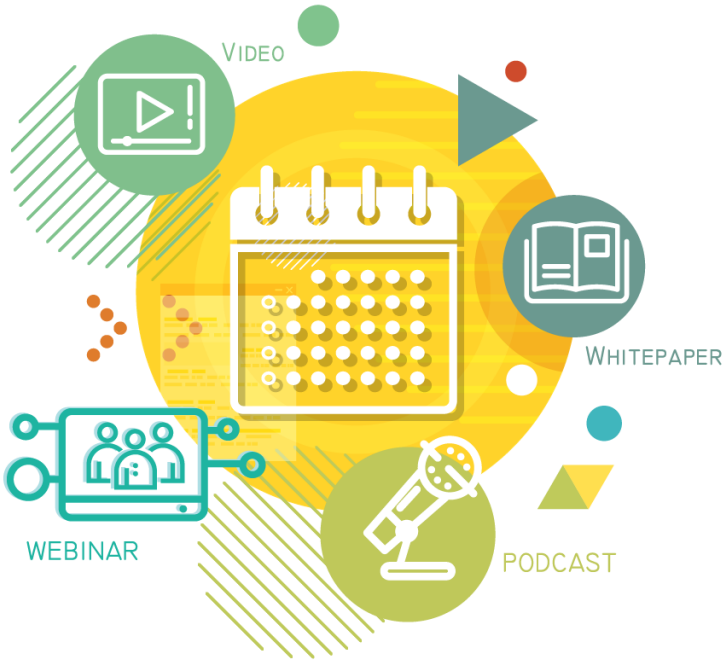
| MONTH | THEME | PRODUCT | LINK |
|---|---|---|---|
| JAN | Insider Risk | Who is the Risk? Game | https://securityawareness.usalearning.gov/cdse/multimedia/games/whoistherisk/story.html |
| FEB | Insider Threat Programs | Cultural Awareness Short | https://securityawareness.usalearning.gov/cdse/multimedia/shorts/int-cultural-awareness/story.html |
| MAR | Workplace Culture | Insider Threat and Equal Employment Opportunity Webinar | https://cdse.acms.com/pgyncwohb32e/ |
| APR | Life Stressors | S2 Vigilance Videos – Episode 2, "Indicators" | https://www.cdse.edu/Training/Security-Training-Videos/Insider-Threat/The-Critical-Pathway-S2-E2-Indicators/ |
| MAY | Personal Resilience | Resilience Animation | https://www.cdse.edu/Training/Security-Training-Videos/Insider-Threat/Resilience/ |
| JUN | Disinformation | Disinformation Stops With You Job Aid | https://www.cisa.gov/sites/default/files/publications/081720_Disinfo%20Toolkit.pdf |
| JUL | Radicalization | Case Study – Jarret William Smith | https://www.cdse.edu/Portals/124/Documents/casestudies/case-study-smith.pdf |
| AUG | Targeted Violence | Targeted Violence Game | https://securityawareness.usalearning.gov/cdse/multimedia/games/kinetic/index.html |
| SEP | Vigilance | S2 Vigilance Videos – Episode 3, "See Something, Say Something" | https://www.cdse.edu/Training/Security-Training-Videos/Insider-Threat/The-Critical-Pathway-S2-E3-See-Something-Say-Something/ |
| OCT | Cyber Insider Threats | Case Study – Victor Grupe | https://www.cdse.edu/Portals/124/Documents/casestudies/case-study-christopher-victor-grupe.pdf |
| NOV | Foreign Collection Methods | The Nevernight Connection | https://www.youtube.com/watch?v=N5V7G9IBomQ |
| DEC | Unauthorized Disclosure | Spillage Poster | https://www.cdse.edu/Portals/124/Documents/posters/small/spillage_v2.pdf |

CDSE Center for Development of Security Excellence

LEARN. PERFORM. PROTECT.

# National Insider Threat Awareness Month (NITAM) 2022

Thanks to everyone for your collaboration on National Insider Threat Awareness Month (NITAM) 2021. There was fantastic engagement from the federal partner community and your participation made this one of the most robust awareness campaigns undertaken by the U.S. Government. Planning is underway for NITAM 2022. You can expect more great content from partners at the National Insider Threat Task Force (NITTF), Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)), Defense Counterintelligence and Security Agency's (DCSA) Center for Development of Security Excellence (CDSE), and the Defense Personnel Security Research Center's (PERSEREC) Threat Lab including campaign guidance, awareness materials, conferences, and events. The 2022 theme will encourage critical thinking to counter malign influence and mis/disinformation campaigns perpetrated by our adversaries. As always, messaging materials and content will include perennial insider threat awareness themes related to awareness and reporting, the role of insider threat programs in proactive risk mitigation, and privacy and civil liberties protections. Programs can pick and choose the messaging and materials that will resonate most effectively within their organization. Campaign materials are updated on the **NITAM website** around the July timeframe to allow time for planning in your departments and agencies. Look for additional updates from the National Counterintelligence and Security Center (NCSC) Enterprise Threat Mitigation Directorate (ETD)/NITTF and the DCSA/CDSE as we get closer to the September launch.




# Advocating For Resources For Counterintelligence and Security Programs

Let's be realistic – asking for more money and resources is not the task that most employees look forward to each year. Yet it is one of the most impactful actions you can take to ensure the appropriate funding and resources are in place to accomplish your department's or agency's mission. The same thing can be said for ensuring that your counterintelligence (CI) and security-related programs are appropriately funded and resourced, especially given that we have all come across what can be considered "unfunded mandates."

There are several basic rules that will enable employees at all levels to assist in advocating for the appropriate CI and security resources:

1) Understand who is involved in your budgeting process. Each department or agency has a different organizational structure and different personnel involved. Leveraging the right people can result in more effective outcomes.

2) Understand how your department or agency budgeting process works and know their deadlines.

3) What is the best way to advocate in order to achieve your budgeting/resource goals within your department or agency? You need to make a good business case as to why you need the resources. This includes answering the who, what, when, where, why, and how questions, and should also note impact – the positive impacts of your CI and security programs and outcomes, and potential negative impacts if your programs are not appropriately funded.

4) Looking for and noting resource opportunities throughout the year. While budget submissions may be due at certain points in the year, compiling notes on issues that must be addressed should happen throughout the year so that you can be ready to have the appropriate conversations regarding your CI and security programs when called upon.

The National Counterintelligence and Security Center (NCSC) can play an important role in helping you position yourself for a successful lobbying effort. Our team works with Intelligence Community (IC) leadership to address National Intelligence Program (NIP) funding. And while NIP funding pertains to IC functions, NCSC can offer advocacy support for CI and security functions such as supply chain security, insider threat, OPSEC, and other CI functions that may fall outside of the IC's purview.

" NCSC can offer advocacy support for CI and security functions such as supply chain security, insider threat, OPSEC, and other CI functions that may fall outside of the IC's purview. "

Lastly, by asking, "What are leadership's priorities?" you can frame your "pitch" in a way that aligns to those priorities. With that in mind, please note that NCSC is dedicated to advocating for resources and budgeting for insider threat, defensive CI, and security programs. We expect that at some point the issues of advocacy and funding will come up in conversations with your leadership and would hope that you are prepared to have those conversations. Remember, you do have the opportunity to impact your department's or agency's mission through the budgeting/resource process…

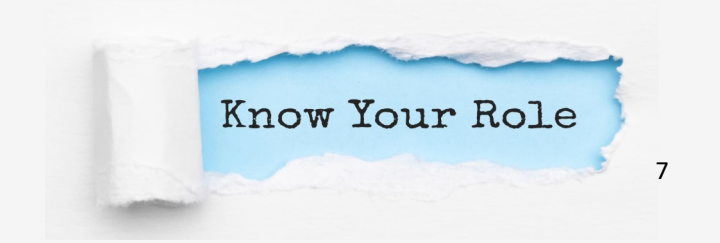
## The National OPSEC Program

As we approach the one-year anniversary of the signing of the National Security Presidential Memorandum (NSPM) 28 that reinvigorated the National Operations Security (OPSEC) Program (NOP) and expanded the OPSEC scope to a whole-of-government approach to protecting our nation, we can take a step back and see how things have progressed for OPSEC over the last year. The execution of NSPM-28 has resulted in unprecedented changes across our nation and forced organizations to evaluate and obtain a deeper understanding of what OPSEC is and how it should be implemented in order to protect our country. The NOP office, under the Enterprise Threat Mitigation Directorate (ETD), has reached out to departments and agencies to ensure they understand their responsibilities under the NSPM-28 and provide access to resources and assistance to support our federal partners in OPSEC implementation. It has been a heavy lift for some departments and agencies, and almost "business as usual" for others who already had an active and progressive OPSEC program in place. In following the requirements of the new national OPSEC policy, the NOP and the National Counterintelligence and Security Center (NCSC)/ETD have worked tirelessly to enhance the national OPSEC program requirements through meaningful interaction, communication, and planning with all stakeholders. These efforts include:

*The upcoming ETD Symposium on January 20, 2022:* This virtual conference will include OPSEC discussions and presentations from subject-matter experts from the Department of Energy and Department of Commerce; and

*National OPSEC Program resources provided by the Interagency OPSEC Support Staff (IOSS):* Virtual instructor-led training, program implementation job aids, computer-based training courses, and other OPSEC-related sessions are available through the IOSS (https://www.iad.gov/ioss).

The IOSS has been an essential element in the transition of the NOP to NCSC, and will continue to provide vital OPSEC training to the community through *December 2022*. As we continue to develop and augment this newly structured NOP office, the focus will continue to be the overall support of all departments and agencies across the nation and encourage those organizations to tap into the wide array of OPSEC training and resources available. Remember, IOSS OPSEC training will discontinue at the end of 2022. Register today for the training that you need to establish your OPSEC program and meet the training needs of your OPSEC practitioners.



# News from The Threat Lab

*Stephanie L. Jaros, The Threat Lab, PERSEREC, DoD*

The Defense Personnel and Security Research Center (PERSEREC) created The Threat Lab in 2018 as a centralized hub for social and behavioral science research related to the counter-insider threat mission space. Since its founding, and with the support of the National Insider Threat Task Force and DoD's Counter-Insider Threat Program, The Threat Lab has expanded to address the professionalization, outreach, education, and training needs of the global counter-insider threat community of practice.

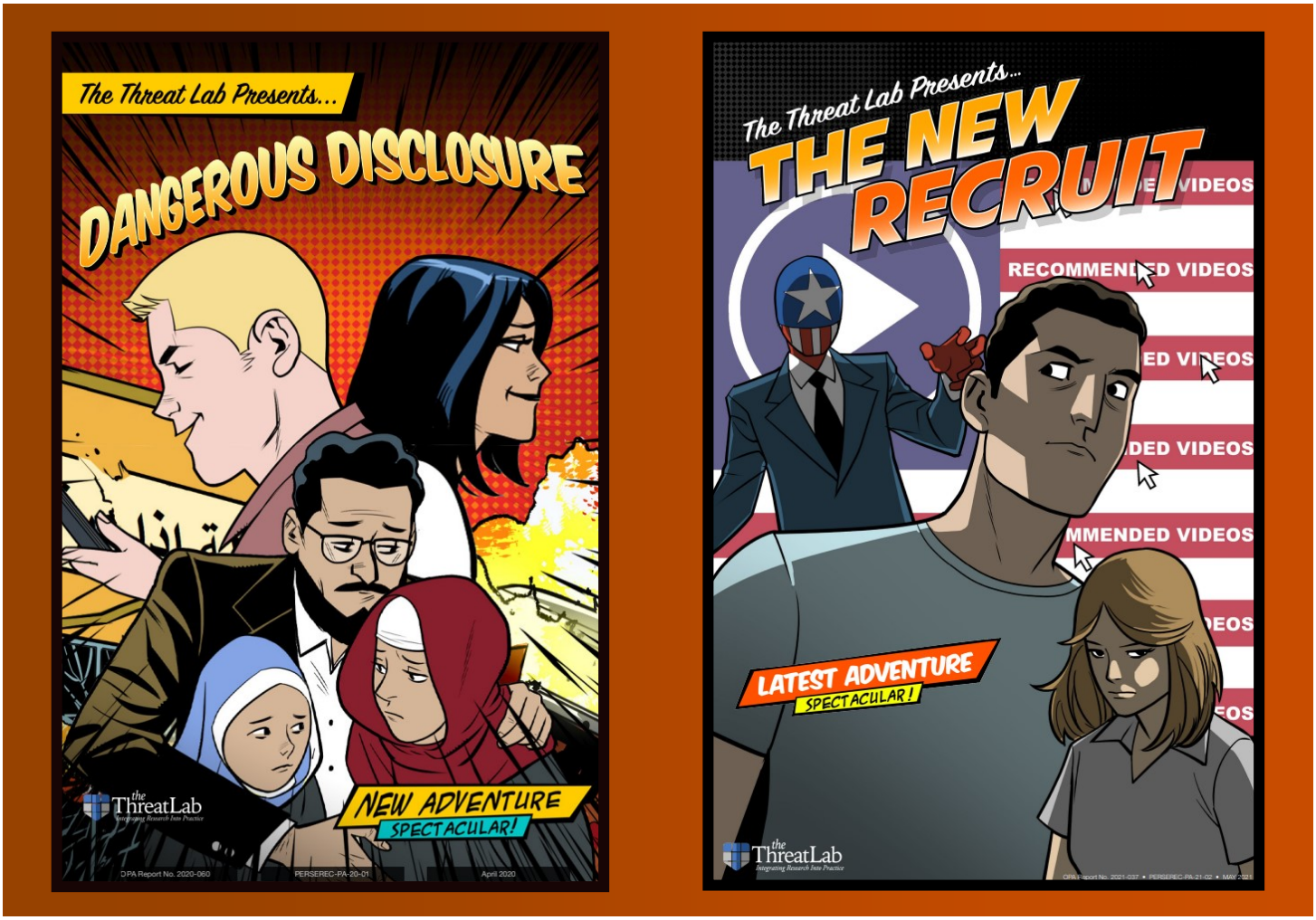
In support of its expanded mission, the team has delivered a number of products and services to both the general workforce and counter-insider threat program personnel. One of The Threat Lab's most successful products has been its annual graphic novel, an initiative led by Dr. David Prina. The first issue, *Dangerous Disclosure*, focuses on the harm that unauthorized disclosures may cause even when no harm is intended. The second issue, *The New Recruit*, tells the story of one person's pathway toward violence, and highlights a number of concerning behaviors that signal opportunities for intervention and assistance.

The Threat Lab encourages counter-insider threat and security professionals to incorporate the graphic novels into their awareness campaigns. Both graphic novels can be found on CDSE's website at https://www.cdse.edu/Training/Toolkits/Insider-Threat-Toolkit/ under the "Research" header and the "Job Aids & Reports" sub-header, or by clicking the images below. The Threat Lab also produced a motion comic version of *Dangerous Disclosure* which can be found at https://vimeo.com/530462391.

To join The Threat Lab's distribution list or to request a briefing, please email DODHRA.THREATLAB@MAIL.MIL.

# Counter-Insider Threat Community Recognition Program

The counter-insider threat community has made great strides in 2021 and we'd like to recognize and share your great work! The National Insider Threat Task Force, the Office of the Under Secretary of Defense for Intelligence and Security Insider Threat Program, and the Department of Homeland Security encourage you to self-nominate for the inaugural Federal Counter-Insider



Threat Community Recognition program by *February 28, 2021*. Categories include Closing Gaps, Detection and Mitigation, Engagement and Collaboration, and Training and Awareness. Our goal is to provide a platform for programs, teams, and individuals receiving this peer recognition to present best practices at an upcoming conference, forum, or other suitable event. For more information on eligibility and how to submit, please contact NITTF-Assistance@dni.gov.

## Counter-Insider Threat Certification News

The Fall 2021 Certified Counter-Insider Threat Professional (CCITP) exam window recently closed, with 32% of candidates taking advantage of Live Remote Proctoring. The National Insider Threat Task Force (NITTF) and Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)) will soon welcome 35 additional professionals into the certified community, totaling 369 CCITP-Fundamentals (CCITP-F) and 121 CCITP-Analysis (CCITP-A) professionals! Certified professionals can now track their professional development units online. For more information visit https://dodcertpmo.defense.gov/Portals/62/PDU%20User%20Guide%20v1%202021.pdf.

The CCITP Program provides a path to obtain recognition for expertise and to demonstrate mastery of U.S. Government established standards in insider threat across Executive Branch departments and agencies. Information on prerequisites, registration, and resources to prepare for the certification exams is available at https://dodcertpmo.defense.gov/Counter-Insider-Threat/.

## Insider Threat Awareness INT101.16 Course Debuts Test-Out Option

*Cashmere He, CDSE, Insider Threat Division*

The Center for Development of Security Excellence (CDSE) Insider Threat Awareness (INT101.16) eLearning course teaches why Insider Threat Awareness is an essential component of a comprehensive security program. CDSE is now offering a test-out option for INT101.16 training. With a theme of "If you see something, say something," the course promotes the reporting of suspicious activities observed at work and teaches the common indicators which highlight actions and behaviors that can signify an insider threat. The course now begins with allowing learners to complete a short test on awareness and basic Insider Threat Awareness skills; those who pass the exam are not required to complete the course content and can proceed to print a Certificate of Completion. Please visit https://www.cdse.edu/Training/eLearning/INT101 to access the course.

## UPCOMING EVENTS

**January - National OPSEC Awareness Month** - NCSC has declared January 2022 as the first annual National OPSEC Awareness Month.

**20 January (9am - 3pm EST)** - Unclassified Virtual ETD Symposium - Guest speakers will be discussing insider threat, defensive counterintelligence, supply chain risk management, and operations security.

**April - National Supply Chain Integrity Month**

**Invitations Coming Soon:**

**17 February** - Enterprise Threat Discussion - Economic Espionage: Behavioral Study on Employee Reporting of Insider Threat Incidents

**March (date TBD)** - Enterprise Threat Discussion - National Counterterrorism Center (NCTC) Information Sharing Initiative

## Resource Corner

**NCSC Website:** NCSC routinely updates our website with the latest information and resources.

**Safeguarding Our Future:** See NCSC's latest fact sheet (12/2021) about protecting your organization from the foreign intelligence threat.

**NITTF Website:** NITTF would love your feedback as we continue to modify this resource to meet your needs.

**IOSS Website:** Establish an account to access IOSS OPSEC training and resources.

**SAGE Website:** To request an account, contact NCSC_FEDS@dni.gov.

**CDSE Insider Threat Catalog:** Training for insider threat practitioners and awareness materials for the general workforce.

**NITTF Directives and Advisories:** See the latest NITTF Advisory 2021-002: Sunsetting the NITTF Hub Operations Course

**ISOO Controlled Unclassified Information:** Training, policy, and other reference materials to support your CUI and Information Security efforts.


# Training and Education Opportunities!

## OPSEC Training

***All course are instructor-led via Microsoft Teams. For more information, or to register, visit www.ioss.gov.***

### OPSEC Analysis Course (OPSE-2380)

**PURPOSE**

This course provides learners with training on how to conduct OPSEC analysis, develop lists of critical information, identify threats and common vulnerabilities, calculate estimated risk, determine viable countermeasures for reducing risk, and brief senior leadership on their findings. Recommended for those involved in OPSEC programs (e.g., program managers, working group members, coordinators, etc.).

**WHEN**

11-12 Jan, 8-9 Feb, 15-16 Mar, 5-6 Apr

### OPSEC Program Management Course (OPSE-2390)

**PURPOSE**

This course provides learners with the knowledge needed to develop and sustain an effective OPSEC program. Learners will be able to identify the required components of an OPSEC program, outline the responsibilities of program managers and coordinators, develop organizational OPSEC policies, and plan internal and external assessments. Recommended for those involved in OPSEC programs (e.g., program managers, working group members, coordinators, etc.).

**WHEN**

13 Jan, 10 Feb, 17 Mar, 7 Apr

### OPSEC and Public Release Course (OPSE-1500)

**PURPOSE**

This course addresses the OPSEC issues that should be considered when reviewing information intended for public release and public access. Learners will be able to edit information to be posted, written, and spoken by applying OPSEC principles, and achieve the originator's objective without compromising critical information. Offered as 1 full-day or 2 half-day sessions.

**WHEN**

18-19 Jan, 15 Feb, 9 Mar, 22-23 Mar

### OPSEC and the Internet Course (OPSE-3500)

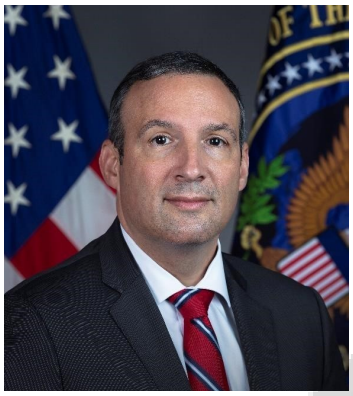
**PURPOSE**

This course introduces OPSEC practitioners to common threats, vulnerabilities, and countermeasures associated with the internet and connected devices.

**WHEN**

24-25 Jan, 16-17 Feb, 29-30 Mar

# A Message From NCSC Leadership



**Michael J. Orlando**
*Senior Official Performing the Duties of the Director of NCSC*

Foreign intelligence threats to the United States are becoming more complex, diverse, harmful, and frequent. Today our adversaries are successfully targeting a broader range of sectors, even those without a direct national security mission or a federal government nexus. Our laboratories, industrial base, academic institutions, and private-sector companies are all at risk. The number of adversaries attempting to obtain sensitive information, research, technology, and industrial secrets by targeting our economy and critical infrastructure is growing.

One year ago, the President signed National Security Presidential Memorandum (NSPM) 28, designating the National Counterintelligence and Security Center (NCSC) as the U. S. Government (USG) lead for operations security (OPSEC). Among other things, the NSPM -28 directs that where appropriate all federal agencies partner with State, Local, Tribal, and Territorial (SLTT) government entities and the private sector to inform and support the integration of the National OPSEC Program (NOP) into their operations and activities. According to the NSPM-28, federal support to SLTT government entities and the private sector should leverage the Intelligence Community (IC) and law enforcement agencies as necessary to help raise risk awareness, identify critical information/indicators useful to our adversaries, and provide risk analysis associated with that information.

*"To be most effective in countering OPSEC threats throughout the country, we must all work as a team to mitigate these threats."*

NSPM-28 encourages federal agencies to coordinate with DHS, FBI, and DOD to identify unclassified and classified OPSEC threat information and mitigation guidance concerning U.S. interests that can be shared with SLTT government entities and private-sector partners. Those SLTT and private-sector partners involved with critical infrastructure, Personally Identifiable Information (PII) of U.S. citizens, and information technologies should be encouraged to coordinate with the NOP, as authorized.

While our federal partners continue to focus on these USG-wide threats, we must remember that a whole-of-government approach that includes SLTT and private-sector partners is necessary to address the overall U.S. OPSEC threat picture. I remind our federal partners of the importance of including SLTT and private-sector partners in their OPSEC endeavors. To be most effective in countering OPSEC threats throughout the country, we must all work as a team to mitigate these threats.

As always, we trust you will find this newsletter beneficial. If you have any suggestions or comments, or topics you would like to see addressed in future issues, please let us know at **NCSC_FEDS@dni.gov**. For more information on NCSC Counterintelligence and security topics, please visit our website at **https://www.NCSC.gov** or follow us on **Twitter @NCSCgov**.

Michael J. Orlando