July 2022 Volume 2 | Issue 3

ENTERPRISE THREAT MITIGATION NEWSLETTER

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

A Message from the Deputy

Rebecca Morgan, NITTF Deputy Director

Rebecca Morgan

"NITAM 2022 will focus on critical thinking skills designed to protect the workforce from foreign malign influence and mis/ disinformation campaigns."

Last fall, the National Insider Threat Task Force (NITTF) initiated the Federal Counter Insider Threat Community Recognition Program with partners from the Office of the Under Secretary of Defense for Intelligence & Security and the Department of Homeland Security Insider Threat Programs. This effort fosters our community of insider threat practitioners by recognizing individuals and teams going beyond requirements to achieve exceptional results. Please join us at the July 21 virtual Enterprise Threat Discussion to recognize your peers and extend congratulations to all of the nominees for outstanding efforts in support of the National Insider Threat Program.

Our July 21 event will also serve as a kickoff for National Insider Threat Awareness Month (NITAM) 2022. Held annually in September, NITAM increases awareness of insider threats and insider risk mitigation best practices. NCSC and the NITTF are working collaboratively with departments and agencies across the federal government to support the fourth annual campaign. In addition to perennial themes related to insider threat awareness and reporting, NITAM 2022 will also focus on critical thinking skills designed to protect the workforce from foreign malign influence and mis/disinformation campaigns. Malign influence and mis/disinformation campaigns represent a profound threat to our trusted insiders. Our workforces require training and support to counter the increasingly sophisticated efforts by our adversaries to exploit our personnel through misinformation, disinformation, and malign influence. Through partnership with stakeholders in the community, we have leveraged a robust body of awareness products, training resources, and other support material to enable implementation of NITAM activities in both public and private sector organizations. By providing access to messaging, tools, and resources in

INSIDE THIS ISSUE

July, we hope to allow plenty of time to plan for an effective September NITAM campaign at your organization. For more information on events and resources, please join us for the virtual Enterprise Threat Discussion on July 21 and/or visit the **NITAM website**.

Over the years, our community partners have embraced NITAM and provided truly amazing awareness campaigns for their workforces. At NITTF and many of our partner organizations, we are also committed to providing training and resources for insider threat practitioners. We recognize that the month can get a bit hectic, but hope you will find time to take advantage of professional development opportunities and celebrate your insider threat program personnel. As insider threat, security, and counterintelligence practitioners, we all encounter a wide range of challenges. Many of us got into this business to detect and deter espionage, but find ourselves confronting issues related to acts of violence, suicidal ideation, child pornography, or other issues of despair. It's important to address the impact of the work performed by our program personnel and provide appropriate outlets and resources.

NCSC/ETD is lucky to work with such a dedicated community of federal partners. We all work hard to support each of you and your programs as you conduct this important work on behalf of national security. Please continue to communicate your requirements, challenges, and successes with our team. We are always looking to improve and support your efforts. And be sure to check out our most recent update to the website. Operations Security resources are now available on the NCSC unclassified "low-side" site. Access training schedules, templates, posters and more at **Operations Security (dni.gov)**, or by going to **www.dni.gov/index.php/ncsc-home** and selecting Operations Security from the "What We Do" drop down menu.

COMMON ACRONYMS

NCSC - National Counterintelligence and Security Center

ETD - Enterprise Threat-Mitigation Directorate

NITTF - National Insider Threat Task Force

NT-50 - Non-Title 50

OPSEC - Operations Security

NOP - National OPSEC Program

IOSS - Interagency OPSEC Support Staff

NSPM - National Security Presidential Memorandum

NCITF - National Counterintelligence Task Force

CI - Counterintelligence

UPCOMING EVENTS

July 21 - Enterprise Threat Discussion - Federal Counter Insider Threat Community Recognition Program & NITAM kickoff

September - National Insider Threat Awareness Month

September - Counter Insider Threat Social & Behavioral Sciences Summit - 30 day virtual event (Registration opens August 1st)

September 1 - CDSE NITAM Conference (Registration POC: Cashmere He - cashmere.c.he.ctr@mail.mil)

September 8 - CDSE webinar - Counter Insider Threat Resources for Your Organization

September 13 - CDSE webinar - Disinformation and Insider Threat

September 15 - Enterprise Threat Discussion - Foreign misinformation, disinformation, and malign influence

September 22 - NITTF hosts virtual Safeguarding Science Seminar

Get your OPSEC products now through September 30th!

Are you in need of products to start your OPSEC Program off on the right foot?

Are you in need of updated OPSEC products for your existing program?

If you answered "yes" to either of these questions, this is the time to take action and order your free OPSEC awareness products from the Interagency OPSEC Support Staff (IOSS)! All OPSEC products available to the community can be ordered through the IOSS website: **https://www.iad.gov/ioss**.

Products are available now through September 30, 2022!

Don't wait! Get them while they last!!!!

The All New DHS Intel Mobile Application

The Department of Homeland Security's (DHS) Office of the Chief Information Officer (OCIO), Office of Intelligence and Analysis (I&A), and the Science and Technology Directorate (S&T) have partnered to bring you the DHS Intel mobile application, an on-the-go way for key leaders, decision makers, and DHS's state, local, territorial, and tribal (SLTT) partners to access and view intelligence produced by Homeland stakeholders across the country.

The DHS Intel app is available to all Homeland Security Information Network (HSIN)-Intel Community members and enables users to view and search for intelligence information, receive alerts when new products are available, and bookmark products for future reference. DHS Intel will continue to evolve with updates and feature enhancements such as improved notifications in the coming months.

The DHS Intel app can be downloaded today through the Apple App Store, or at this link **(https://apps.apple.com/app/id1614493429)**. It will be available on Google Play this summer.

Keeping Safe on Social Media

Developed by the National Security Agency (NSA) in 2021, the Cybersecurity Information Sheet entitled: *Keeping Safe on Social Media*, is a brief guide that highlights critical information and countermeasures users may take to help keep themselves and their sensitive date safe while connecting with others on social media.

The *Keeping Safe on Social Media* information sheet provides a few safety tips, as well as OPSEC guidance for using Social Networking Sites (SNS). SNS, like Facebook® and Twitter®, are software applications that connect people and information in spontaneous, interactive ways. While SNS can be useful and fun, they can provide adversaries, such as terrorists, spies, and criminals, with critical information needed to harm you or disrupt your mission. Practicing good OPSEC on social media will help you to recognize your critical information and protect it from an adversary.

To view the *Keeping Safe on Social Media* document, please visit

https://media.defense.gov/2021/Sep/16/2002855950/-1/-1/0/CSI_KEEPING_SAFE_ON_SOCIAL_MEDIA_20210806.PDF

Content in this document was provided by the Interagency OPSEC Support Staff (IOSS).

For more information about IOSS, please visit **https://www.iad.gov/ioss**.

" Protecting classified information from unauthorized disclosures is the responsibility of every cleared employee. "

Protecting Classified Information From Media Leaks

Every U.S. Government department and agency with staff or contractors who handle classified national security information should have procedures in place to detect, prevent, and respond to suspected unauthorized disclosures to the media or other public forums on the Internet.

In most cases, the staff and contractors who handle classified information are best positioned to identify classified information that appears in media or internet forums. Not all items flagged by these subject matter experts turn out to be new unauthorized disclosures. Nevertheless, departments and agencies with classified material need to ensure that cleared staff and contractors are alert to suspected unauthorized disclosures, and know how to report suspected items to the relevant office of security. Departments and agencies also need procedures to report such suspected unauthorized disclosures as appropriate for further investigation and potential prosecution. For the 18 departments and agencies in the Intelligence Community, procedures for reporting are covered in Intelligence Community Directive 701. Security staffs in other departments and agencies also should be attentive to these procedures and their own agency-specific requirements.

As part of preventing unauthorized disclosures of classified information, departments and agencies should raise awareness among staff and contractors of the consequences of such disclosures. All cleared individuals have an obligation to protect classified information. Failure to do so can result in damage to national security. Leaks of classified information to the media and wider internet forums risk neutralizing intelligence sources and methods, as well as providing rich, no-cost collection opportunities for Foreign Intelligence Entities.

Departments and agencies need to ensure that staff and contractors who handle classified national security information are clear on their responsibilities for protecting that information, regardless of their personal, ethical, or political views or grievances. With diligent reporting, the consequences of unauthorized disclosure can be mitigated.

Every clearance holder has recourse to approved whistleblower processes as one of the key means of ensuring government accountability. There are approved channels to report fraud, waste, or other abuse through existing whistleblower or inspector general channels. There are also approved channels for the release and review of government information. The Whistleblower Protection Act and Presidential Policy Directive 19 (PPD-19) protect employees from direct retaliation for acts of reporting protected disclosures. They do NOT protect employees who unlawfully disclose classified information. Security programs must work with their cleared personnel to clarify the difference and learn where and how to report both unauthorized disclosure and questionable government behavior and activities.

Protecting classified information from unauthorized disclosures is the responsibility of every cleared employee. Our defenses are only as good as the procedures we have in place to detect, prevent, and respond to unauthorized disclosures.

Items Prohibited in Federal Facilities – 2022 Updates

Interagency Security Committee (ISC)

On June 1, 2022, the Interagency Security Committee (ISC) released its update of ***Items Prohibited in Federal Facilities: An Interagency Security Committee Standard, 2022 edition*** to establish guidance to protect facility occupants and visitors from items that are dangerous, unlawful, or otherwise determined to create vulnerabilities in safety and security. Further, it establishes a list of prohibited items and procedures to control them, increasing consistency in approach and preventing confusion at screening checkpoints.

UPDATES IN THE 2022 VERSION INCLUDE

- Documentation requirements
- Inclusion of training aids as controlled items
- Prohibited Items Exemption Request Form/Template

Consistent with Executive Order (EO) 12977, the new Standard identifies a baseline list of prohibited items that each responsible authority shall customize to mitigate facility risk. It is applicable to all executive branch buildings and facilities in the United States occupied by federal personnel for non-military activities. These facilities include currently owned, to be purchased, or leased facilities; standalone facilities; federal campuses; and, where appropriate, individual facilities on federal campuses and special-use facilities. Additionally, per Department of Defense (DoD) Instruction, 2000.12, all DoD leased facility space or space in buildings owned or operated by the U.S. General Services Administration (GSA) not located on DoD property must comply with this standard.

For more information about the ISC, please visit the ISC home page.

INTERAGENCY SECURITY COMMITTEE

Items Prohibited in Federal Facilities

An Interagency Security Committee Standard

2022 Edition

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency
Interagency Security Committee

"[Items Prohibited in Federal Facilities: An Interagency Security Committee Standard] is applicable to all executive branch buildings and facilities in the United States occupied by federal personnel for non-military activities."

Farewell to the IOSS and the Purple Dragon

After 34 years, the Interagency OPSEC Support Staff (IOSS), responsible for running the National OPSEC Program (NOP), under the executive direction of the Director, National Security Agency, has transitioned to the National Counterintelligence and Security Center (NCSC). As a result of the signing of NSPM-28 on January 13, 2021, the IOSS started making plans to transition the mission to NCSC and has continued to work diligently to support the knowledge transfer and all other components over to their new home. As of December 31, 2022, the IOSS will no longer be in existence, but the National OPSEC Program will continue to flourish under the direction of the Enterprise Threat-Mitigation Directorate within NCSC.

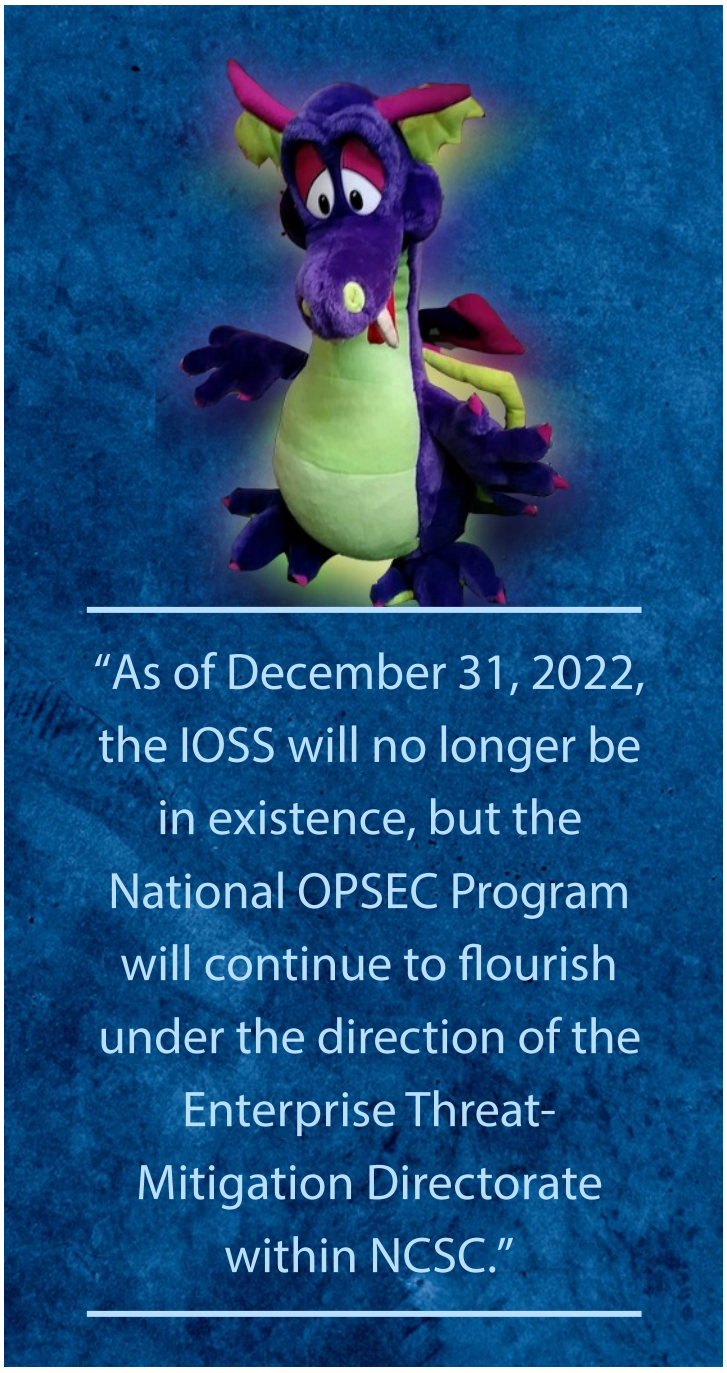
Throughout its history, the IOSS and its many staff members have enjoyed promoting and defining the National OPSEC Program efforts for various organizations and agencies across the nation. Support has been provided to the community through publications, awareness products, training courses and resources, assessments and consultations, and hosting numerous National OPSEC Conferences and Symposiums, with attendees ranging from 350 – 1000 at its peak. The IOSS has built a strong multi-faceted organization based on mutual mission focused support and a strong sense of community and passion for protecting our nation.

Since its inception, the IOSS has advocated for countless OPSEC professionals and organizations associated with operations security through continuous partnerships and interaction throughout the community. OPSEC programs worldwide have been built, fostered, and thrived, becoming mainstays at organizations across the U.S. Government.

Joining us halfway through our tenure was "CESPO" (OPSEC spelled backwards) The Purple Dragon, who became the unofficial mascot of the IOSS. He spent much of his time greeting attendees at our exhibits and conferences or hanging out taking selfies. He, along with many of the holdings of the IOSS, will now spend their time representing the national mission and IOSS at NSA's National Cryptologic Museum.

Everything IOSS members accomplished over 34 years could not have been realized without those who came before us. To the original Purple Dragon Team who identified the need for OPSEC during the Viet Nam War era, we extend our great respect and gratitude. Dedication to their craft paved the way for all that we have accomplished and continues to influence today's OPSEC practitioners throughout the world.

As the IOSS fades into the past, we would like to thank everyone who has supported our efforts in some way, and those who have been proactive in their mission to promote OPSEC principles over the years. Our sincere thanks for all who have supported us throughout our existence include speakers, practitioners, support personnel, event planners, and all that worked behind the scenes. We send our best wishes to those yet to come and hope our contribution will continue to make a meaningful difference in the pursuit of OPSEC! We offer a resounding round of applause to everyone who was and will be an advocate of practicing and promoting OPSEC to keep not only our nation, but our families, safe for years to come!



Federal Counter Insider Threat Community Recognition Program Selectees

Last fall, the National Counterintelligence and Security Center, Enterprise Threat Mitigation Directorate (NCSC/ETD), National Insider Threat Task Force (NITTF), the Office of the Under Secretary of Defense for Intelligence & Security (OUSD(I&S)) Insider Threat Program, and the Department of Homeland Security (DHS) Insider Threat Program initiated the Federal Counter Insider Threat Community Recognition Program. The program fosters a community of insider threat practitioners by recognizing individuals and teams throughout the U.S. Government that go beyond requirements to achieve exceptional results while supporting leadership objectives of the U.S. Government Counter Insider Threat Program.

The community responded robustly. Please join us in congratulating the below selectees and thanking them for their exceptional contributions to the insider threat community!

We are also delighted to congratulate **Megan Davey**, DHS; **Anthony Saputo**, NITTF; and **Tim Davis**, DoD Liaison to NITTF, who earned honorary recognition.

We would also like to extend congratulations to all of the nominees for outstanding efforts in support of the national insider threat program. We appreciate their participation and enjoyed reading about all the significant achievements throughout the year.

We hope you'll join us on **July 21** to recognize the selectees at the monthly NCSC Enterprise Threat Discussion, which will also feature a kick off for National Insider Threat Awareness Month 2022. To register for the event, please reach out to **ETD-REGISTRAR@dni.gov.**

SELECTEE	CATEGORY	DEPARTMENT/AGENCY
INSCOM Security Operations Center	Closing Gaps	Department of the Army
Justice Management Division Insider Threat Center	Closing Gaps	Department of Justice
Nicholas Vallero Kimsey	Closing Gaps	Transportation Security Administration
Casey Stuart Rowland	Detection and Mitigation	US Army
Risk 360 APEX Team	Detection and Mitigation	National Geospatial-Intelligence Agency
Insider Threat Program	Engagement and Collaboration	Department of State
Dr. Seth A. Bridges	Engagement and Collaboration	National Geospatial-Intelligence Agency
Carla Dawn Stamper	Training and Awareness	Army Insider Threat Program
NITAM Team	Training and Awareness	National Geospatial-Intelligence Agency

NOMINEE	DEPARTMENT/AGENCY
Boone and Griffith	Department of the Army
Callie J. Chandler	Defense Personnel and Security Research Center
Counter Insider Threat Program	Defense Information Systems Agency
Defense Personnel and Security Research Center	Defense Human Resources Activity
DISA Insider Threat Team	Defense Information Systems Agency
Insider Threat Deterrence Team	Department of State
Insider Threat Division Mitigation Team	Defense Intelligence Agency
ITP Detection and Mitigation Team	Department of State
Joshua E. Reese	Department of the Air Force
Justice Management Division Insider Threat Center	Department of Justice
Justice Management Division Insider Threat Center	Department of Justice
Liza Briggs and Laurel McKenzie	USMC
Michael G. Tirrell	DHS ICE
TRADOC G2X	US Army
Treasury Insider Risk Management Office Team	U.S. Department of the Treasury

The State of Enterprise Threat Mitigation: 2021 Annual Report

In May 2022, the Enterprise Threat-Mitigation Directorate (ETD) released *"The State of Enterprise Threat Mitigation: 2021 Annual Report."* The report summarizes the 2021 activities of the NCSC/ETD to strengthen executive branch programs addressing insider threat, operations security (OPSEC), unauthorized disclosure, and defensive counterintelligence program development. This report discusses ETD's engagement with the federal community, Intelligence Community (IC), and Department of Defense (DoD) components, including outreach, training, and technical assistance to foster program maturity.

A copy of the U//FOUO report can be made available to those with .gov or .mil email addresses. Please contact ETD-Assistance@dni.gov to request a copy of the U//FOUO version. In addition, a classified version is available to those with the appropriate clearances at www.ncsc.ic.gov/etd/resources.

2022 National Intelligence Professional Awards Program

In 2007, the Intelligence Community Directive (ICD) 655 established a National Intelligence Awards Program (NIAP) consisting of National Intelligence Community Awards (NICAs) and National Intelligence Professional Awards (NIPAs). The NICAs and NIPAs consist of non-monetary and monetary honorary awards to recognize distinguished service or exceptional contribution to the U.S. Intelligence Community (IC).

On August 11, 2022, on behalf of the IC Senior Program Executives, the NCSC will present the NIPAs to those in the IC who, through exceptional accomplishments or service, enhance the standing and stature of professions, functions, and disciplines that support the counterintelligence (CI) and security missions and the advancement of the missions and objectives set forth in the National Intelligence Strategy of the United States of America. This year, NCSC will also recognize the highest achievements of an individual and/or team with the NCSC Director's Award for Excellence.

The Talent Development Group from NCSC's Mission Integration Directorate received numerous award packages this year from the IC. The packages were forwarded to a Review Board comprised of senior level CI and security subject matter experts from across the IC who focused on evaluating the submissions. The packages were reviewed and rated using the following criteria: 1. Innovation, Creativity, and Originality, 2. Integration and Information Sharing, and 3. Impact.

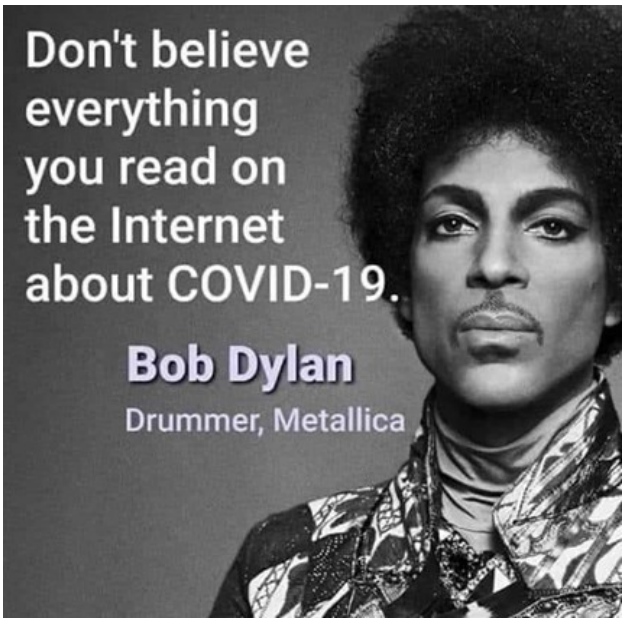
Nine individuals and 14 teams were selected this year from the 12 categories below. We would like to thank all departments and agencies that submitted nominees for this years awards program and note that the next call for nominations will be announced on September 1, 2022.

Awards Categories			
Counterintelligence Operations	Counterintelligence Analysis	Insider Threat Detection	Information Security
Counterintelligence Investigations	Countering Technical and Cyber Threats	Personnel Security	Industrial Security
Counterintelligence Collection	Education/Training	Physical and Technical Security	Supply Chain Protection

Critical Thinking and Mis/Disinformation

Let's be realistic - the more time you spend on the Internet, the greater the chance you'll run into misinformation and/or disinformation. False or misleading information can be in the form of almost anything: memes, news articles, pictures/graphics, white papers, statistical analysis, speeches, etc., and can potentially come from any source.

Take this meme, which one would hope was constructed under the guise of humor: the statement itself is reasonable (i.e., no, you shouldn't believe everything you read on the Internet about COVID-19), but for those of you who are not aware, everything else about this meme is questionable:



1) Bob Dylan probably never said that.
2) Bob Dylan isn't known for his drumming.
3) He never played for Metallica.
4) That's a picture of Prince.

Additionally, some of you may remember the State Farm commercial from almost 10 years ago where two people are talking and the conversation goes something like this: "They can't put anything on the Internet that isn't true…Where did you hear that?…The Internet."[1] And before the Internet, mis/disinformation was promulgated through media such as TVs, radios, and newspapers. It's always been there – but with the Internet it's never been easier for the average person, foreign intelligence entity, business, government, or politician to promulgate mis/disinformation directly to unsuspecting recipients around the world.

Laws, core values, operating principles – those things don't dictate whether something is true or not, or whether the person providing the information is trustworthy/credible or not. So what can you do to combat mis/disinformation? Along the lines of "trust but verify", you can take steps to minimize the impact of mis/disinformation, including:

1) Whatever the source, do your own research
2) Determine if the info you find aligns with what you are being told
3) Just because someone is right about x doesn't mean they are right about y
4) Parse every word
5) Note that opinions are just that: opinions[2]
6) Ask the who, what, when, where, why, how questions that will give you the answers you need to form an informed opinion
7) Don't believe everything you hear
8) On the other hand, don't be paranoid
9) Be aware of fallacies and other ways that information and/or people can be manipulated

Here is a critical thinking exercise for you: Most people have heard of the concept of best practices – but what are best practices? Are they the best practices that the people who are noting them as best practices have found, at least up to this point? Who says they are best practices? Are they best for your organization? Do you have any already established practices that are getting good results for you (i.e., that YOU would consider to be best practices)? What are good results or how do you define "good results" – compliance with statues and department/agency policies, provide useable data, etc.? All these questions, and more, arise from a simple question of what is a best practice.

Here is another critical thinking exercise: Misinformation and disinformation about crime and violence in the U.S. is extensive, with one of the primary modes being the use of crime statistics to make a political point. Cherry-picked statistics and facts may be true, but in the overall context, are they misleading? While there are a number of sources for that type of information, the Federal Bureau of Investigation (FBI) publishes crime stats that are broken down by a number of different categories: UCR Publications — FBI. Should you trust this source? Should you trust other sources such as the Centers for Disease Control (CDC) or any one of a number of aggregators or private sector analysis of crime stats? Should you trust sources that use the information from the FBI but only use certain pieces of information?

Lastly, there are many resources on the topic of fallacies. While there seems to be too many fallacies to count, familiarizing yourself with the different types of fallacies may enhance your ability to critically think through ideas, issues, concepts,

processes, or any other content where accepting what you see or hear without question may not be the most prudent path forward.

You may find that maintaining vigilance (some may say cynicism) over everything you read can be mentally draining - it can feel like an exercise in frustration at times. But the alternative is being tricked and cajoled into believing a false reality. That doesn't serve you, your organization, or our nation well.

[1] In Youtube, search "State Farm French Model"

[2] Opinion: a belief based on experience and on certain facts but not amounting to sure knowledge

ODNI/FSLTT is on the Homeland Security Information Network (HSIN)-Intelligence Platform

In an effort to ensure that data and intelligence from the ODNI is readily shared and available, the Federal State, Local, Tribal, and Territorial (FSLTT) Partnerships Group created a presence on the Department of Homeland Security (DHS) Homeland Security Information Network (HSIN)-Intelligence platform. HSIN is the DHS official system for trusted sharing of Sensitive But Unclassified information between federal, state, local, territorial, tribal, international, and private sector partners. With a majority of Non-Title 50 (NT-50) Executive Branch agencies and organizations operating within the UNCLASSIFIED environment, this platform will allow for more exchange of valuable and timely data and intelligence. The FSLTT Partnerships Group encourages the collaboration of various products with our NT-50 Federal Partners to ensure vital missions and goals are accomplished through such coordinated efforts and platforms such as HSIN-Intel. HSIN access is based on nomination and acceptance into one or more HSIN communities. For more information about HSIN, or to learn how you can join HSIN, please visit **https://www.dhs.gov/homeland-security-information-network-hsin.**

//

"The FSLTT Partnerships Group encourages the collaboration of various products with our NT-50 Federal Partners to ensure vital missions and goals are accomplished through such coordinated efforts and platforms such as HSIN-Intel"

Training and Education Opportunities!

OPSEC Training

All courses are instructor-led via Microsoft Teams. For more information, or to register, visit https://www.iad.gov/ioss.

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

16-17 August, 20-21 September

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

18 August, 22 September

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 one full-day or two half-day sessions.

WHEN

25-26 July*, 23 August, 13-14 September*

Note: *= Two half day (4 hour) sessions

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

20-21 July, 17-18 August, 21-22 September

Note: Each class is two half day (4 hour) sessions

Senior Official Performing the Duties of the Director of NCSC

Michael J. Orlando

During September 2022, the Office of the Director of National Intelligence's National Counterintelligence and Security Center will work collaboratively with departments and agencies across the federal government to support the fourth annual National Insider Threat Awareness Month, which emphasizes the importance of safeguarding our nation by detecting, deterring, and mitigating insider risk.

Our trusted workforces (our insiders) are some of the most valuable assets in our nation, but they face an increasingly challenging risk environment. From the disruptions to work and home life wrought by the global pandemic, to adversary efforts to co-opt or exploit vulnerable employees, the risks for espionage, violence, unauthorized disclosure, and even unwitting insider threat actions are higher than ever. 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.

> *"Maintaining effective insider threat programs is critical to supporting our workforces and reducing their vulnerabilities."*

Maintaining effective insider threat programs is critical to supporting our workforces and reducing their vulnerabilities. As you know, pursuant to Executive Order 13587, all federal departments and agencies are required to maintain a program to deter, detect, and mitigate insider threats. Insider threat programs are comprised of multidisciplinary teams that address threats while protecting the privacy and civil liberties of the workforce, maximizing organizational trust, and ensuring positive workplace cultures that foster diversity and inclusion. Insider threat programs also provide an array of resources to support public and private sector organizations, decreasing vulnerabilities and increasing the resilience of their valued personnel.

Participating in National Insider Threat Awareness Month will help public and private sector organizations more effectively deter, detect, and mitigate insider threats by increasing awareness and promoting reporting. Most insider threats emerge over time, with concerning behaviors evident prior to negative workplace actions. Insider threat awareness is not about curtailing free speech or suppressing legitimate whistleblowing, but about recognizing and reporting behaviors of concern to provide opportunities for early intervention, leading to positive outcomes for at-risk individuals and reduced risk to organizations.

I look forward to your participation in National Insider Threat Awareness Month this September and encourage you take advantage of the many tools and resources that will be made available. There are many ways to get involved. For a list of events and resources as well as suggestions for activities at your organization, please visit **securityawareness.usalearning.gov**.

Michael J. Orlando