April 2022 Volume 2 | Issue 2

ENTERPRISE THREAT MITIGATION NEWSLETTER

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

A Message From ETD's Assistant Director

Robert Rohrer, NITTF Director & ETD Assistant Director

The National Institute of Standards and Technology (NIST) Special Publication 800-39 provides a formal definition of "Advanced Persistent Threat" (APT), describing APT as sophisticated, resourced, and enduring adversarial threat. At its core, APT is a human threat, with threat actors or their agents seeking to achieve the adversary's objectives. The last point- that APT is focused on human objectives- is most important.

As described in the *2020-2022 National Counterintelligence Strategy of the United States*, we face an ever-increasing threat from great power competitors. Our most sophisticated adversaries use all traditional and non-traditional intelligence capabilities, as well as proxies, to achieve their strategic objectives. Those objectives target all of our national and economic security assets and resources. It does not matter if our high value assets are government people or information, the trade secrets of our private sector partners, or our critical infrastructure. If it serves the APT's strategic objectives, our great power competitors will simply not stop until they succeed.

In response to this increasing threat, National Security Presidential Memorandum (NSPM) 28 expanded the National Operations Security (OPSEC) program and requires the adoption of the OPSEC cycle (a risk management model) by all federal departments and agencies. In essence, this means that all departments and agencies must include foreign adversarial threat (the greatest APT we face) into organizational risk management practices, and apply appropriate countermeasures. NSPM-28 moves the National OPSEC Program well beyond the traditional military concept of OPSEC, and requires the whole-of-government to protect all governmental resources from adversarial exploitation. Further, NSPM-28 requires federal agencies promote OPSEC practices to all our partners, especially our supply chain.

This month, we renew our efforts to protect America's supply chain. As we do so, it is important to remember that APT is not technical. The APT is human. It is intelligence. It is orchestrated. It is unwavering. And in the case of our great power competitors, the APT will create vulnerabilities, even where they do not inherently exist, anywhere in the supply chain.

This month I want to encourage all of our partners to participate in National

INSIDE THIS ISSUE

Supply Chain Integrity Month, especially those not directly involved in Supply Chain Risk Management. To counter our adversaries' ability to migrate across threat vectors, it is more important than ever that counterintelligence and security professionals from all disciplines have a robust understanding of each others' roles and responsibilities.

UPCOMING EVENTS

April *- National Supply Chain Integrity Month*

May *- Mental Awareness Month*

June *- National Internet Safety Month*

20 April - *Supply Chain event* - NCSC Open Source Software - An International Discussion

21 April - *Supply Chain event* - Georgetown University hosted panel discussion with government and private industry

26 April - *Supply Chain event* - INSA Keynote Speaker

26 April - *Supply Chain event* - NASA Webinar

28 April - *Supply Chain event* - CDSE Webinar - Semiconductor Supply Chain

28 April - Enterprise Threat Discussion - Best Practices of Supply Chain Security and Resiliency

5 May - NCITF CI Educational Series - NT-50 Day

May (date TBD) - Enterprise Threat Discussion

June (date TBD) - Enterprise Threat Discussion

For more information on upcoming events, please contact your ETD/NITTF liaison officer.

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

How Identity Fraud Creates a Security and Insider Threat Risk

The increasing use of technology to advance business operations has been a boon to departments, agencies, and the private sector, particularly in addressing communications shortfalls related to the COVID-19 pandemic. But the use of technology has also introduced a variety of security vulnerabilities in various areas of business practice, from hacked video-conferencing meetings, to ransomware and phishing schemes. This article addresses an increasingly frequent scam which not only embarrasses a company, department, or agency, but creates a tremendous risk: identity fraud during the hiring process.

Industries such as computer and technology are notorious for high staff turnover and a need to hire well educated, experienced, and technically competent personnel. Video conferencing is a great way to conduct interviews quickly and efficiently with less disruption to recruiters, hiring managers, and staff involved in the vetting process. But imagine finding the perfect fit for your open position, whom you hire by leveraging all the remote tools such as an emailed and digitally signed offer and contract. They arrive and begin working onsite, or, worse, begin working remotely with the laptop, personal identity verification (PIV) card, and phone you sent to them. After a couple of days, someone begins to realize the person who just on-boarded is not the same person you interviewed remotely. Worse yet, you have given this person direct access to your computer systems, which house your sensitive, proprietary, or classified information. In imposter fraud, an individual has represented themselves as a candidate at the behest of someone else. The imposter is typically a more articulate and accomplished interviewee, likely possessing an exceptional grasp of the content area of the position at hand. For example, a computer programmer with limited experience using Linux might hire another person to interview on their behalf who has extensive Linux programming experience. Upon being hired, the "real" candidate reports for work.

> *"Although it is not a common fraud scheme, the damage that an unknown individual, hired under false pretenses, can do as an insider threat is tremendous."*

Although it is not a common fraud scheme, the damage that an unknown individual, hired under false pretenses, can do as an insider threat is tremendous. The damage may include theft of information, intentional sabotage of your computer systems, or even unintentional degradation of your work products due to lack of relevant skills to do the job they were hired for. Additionally, anyone willing to engage in this type of fraud is an established rule breaker and has engaged in criminal activity.

Issues like these are why the National Insider Threat Task Force and Enterprise Threat-Mitigation Directorate promote a holistic approach to threat mitigation, where human resources, legal, and other functional groups play a role in your organization's risk mitigation process. In these cases, human resources personnel are the first line of defense to ensure that the right people are hired. And if someone who committed identity fraud slips through the cracks but is discovered after being hired, human resources and legal counsel have roles to play in resolving the employment-related issues, while your information technology and security personnel would be responsible for analyzing all the networks and materials that were accessed.

A proactive approach to the issue of identity fraud would include looking at your hiring and onboarding process to see what vulnerabilities and gaps exist that could allow for fraud or deception to take place. Among the steps that can be taken to help mitigate fraud risk in remote hiring are; 1) taking a screenshot of the individual being interviewed and cross-checking with the individual who reports on day one for work, 2) being diligent in interviewing prior employers and references carefully to determine if the candidate's listed abilities match up with their past experience and performance, 3) establishing the candidate's identity by having them produce photo identification (driver's license, passport, government issued work permit) at the start of each remote interview, and 4) ensuring your organization is prepared to civilly and/or legally pursue identified cases of fraud. Warning candidates of this intent verbally and in writing is not a bad practice either.

Threat Mitigation: A Fusion of Security Disciplines

Ken Collins, Environmental Protection Agency (EPA) Insider Threat/OPSEC Program Manager

On January 13, 2021, the President signed National Security Presidential Memorandum (NSPM) 28, the *National Operations Security Program* (NOP), which updates National Security Decision Directive (NSDD) 298, *National Operations Security Program*, issued in 1988. NSPM-28 charges agencies with funding and maintaining its organizational OPSEC programs commensurate with the scope of their national security missions and responsibilities and the level of presented risk. It is a security discipline focused on a risk-based, comprehensive, whole-of-nation effort.

How can smaller Non-Title 50 (NT-50) programs more efficiently support this new mandate? By combining internal resources, creating a "Security Fusion Enterprise" or "Blended Security" function within their respective agency. As you read through the guidance provided in NSPM-28, you will see similar requirements to those in Executive Order 13587, *National Insider Threat Policy*, as well as the *Minimum Standards for Executive Branch Insider Threat Programs*. Some of the similarities include an agency-appointed Senior Designated Official (SDO), Program Manager (PM), functioning working group, and initial and annual awareness training. Hopefully your agency already has these functions in-place for their insider threat program. If so, utilizing many of the same key agency personnel could be a solution.

While NSPM-28 does not specifically instruct an agency on how to implement OPSEC within their agency, one approach could be to utilize existing insider threat organizational structure, staffing, and resources to accomplish the task. Not only would this allow for the sharing of resources but would also enhance communication efforts and unify mitigation practices. Your insider threat SDO and PM could also serve as your OPSEC SDO and PM. Analytical functions currently being performed by

"Security needs will continue to grow at a faster pace than resources thus requiring agencies to adapt security-in-depth practices."

insider threat team members could also be performed for OPSEC. Existing insider threat awareness training could be modified to include OPSEC awareness (if not already being accomplished in your organization). Depending upon your organization's needs, additional staffing may need to be considered to fulfill these roles, which would benefit both programs. Other security disciplines such as Counterintelligence and Supply Chain Risk Management could also be fused into a threat mitigation function. Which security disciplines to incorporate will be dependent upon your agency's needs, resources, and configuration.

One advantage of having fused or blended security disciplines functioning as a threat mitigation discipline is command and control. Duplication of efforts would be all but eliminated ensuring resources are being utilized efficiently. If there are numerous security disciplines all assessing the same incident, there will surely be varying courses of action taking place. This could cause confusion which could jeopardize the outcome of the inquiry.

In conclusion, security needs will continue to grow at a faster pace than resources, thus requiring agencies to adapt security-in-depth practices. Blended or fused threat-mitigation, coupled with a trained workforce, is one cost-effective solution. Just note that what works best for a particular agency may not for another. You should assess vulnerabilities through a holistic, security approach, encompassing several security disciplines throughout the process.

OPSEC Requirements for Foreign Visitors and Assignments

Paul Ruehs, Security Programs Manager, Department of Energy, Office of Headquarters Security Operations

Hosting a foreign visitor is a critical responsibility. Many government and supporting contractor facilities are involved in some type of research and development activities. Others routinely use or have access to new advanced technologies. In order to discover new technologies, government entities often seeks individuals or programs from other countries with the desirable scientific and technical skills to participate in cooperative and joint ventures. These visits and joint activities advance your department's missions consistent with U.S. national security policy and objectives.

There is an inherent risk with site visits, assignments, or other associations with foreign nationals. Individuals, working on their own or on behalf of foreign intelligence entities or commercial enterprises, advance their self-interests by economic means. They compete in today's race for international economic strength and influence. Visits/assignments to government facilities often provide foreign countries a low cost opportunity to access needed technologies. Information doesn't have to be classified to be of value and desirable. In fact, unclassified information is often targeted because it is generally more accessible, easier to obtain, and may not be available to the visitor at home. Indeed, so important is unclassified but sensitive data, there is an intelligence discipline known as Open Source Intelligence (OSINT) that is part of our other collection activities.

The OPSEC Program is an important facet in protecting sensitive information. Prior to the arrival of a foreign national, an OPSEC review should be conducted to ensure information is protected. The assessment must address potential OPSEC vulnerabilities and necessary countermeasures. These reviews ensure that the required security plan is adequate.

The OPSEC review should include the facility/location, programs, information, and technologies, to include facility access and affiliated activities, bulletin boards, and what can be observed that may allow the visitor access to material they are not authorized to see. At a minimum, the review should focus on security disciplines such as physical security, information security, and cyber security. This especially applies to your office's information technologies (IT) systems. Be especially cautious when allowing a visitor access to your systems.

It is imperative that your agency's critical information be identified and hosting/escorting officials are familiar with your critical information. Critical information includes those classified or sensitive unclassified areas, activities, functions, data, or information about an activity or organization deemed sufficiently important to be protected from an adversary. Examples of critical information that must be protected include personnel files, proposal and contract documents, or financial data regarding a project. Operations, research and development initiatives, and security activities and requirements are other examples of data that must be protected. Good OPSEC requires each agency/activity to maintain a current critical information list (CIL) of their sensitive information. Usually, your facility security officer (FSO) or OPSEC representative would keep the CIL. Incidentally, all employees should be familiar with their organization's CIL. After all, how can you protect what you don't know you are required to protect?

The OPSEC representative plays a critical role in the hosting process. Key actions include being involved in the approval process for foreign national visits, being involved during the visit, and ensuring training programs are in place.

But why the concern?

Once in a facility, good collectors can manipulate the visit to address some or all of their collection requirements – think OSINT. Some visiting foreign scientists or engineers may take advantage of the situation to take acquired technology back to their own country and apply it directly to their needs without having to wait for it to arrive through a bureaucratic intelligence collection process. It is not out of the realm of possibility that many countries use scientists and technology experts as collectors and intelligence operatives. What better cover for a spy who is "dual hatted" to be part of an exchange program or research and development joint initiative? Signs include wandering visitors, inappropriate questions, taking photographs, and last minute additions to visiting delegations.

What Can You Do? - Security Countermeasures

Some recommended security countermeasures to mitigate vulnerabilities associated with these collection techniques are relatively simple, inexpensive, and effective. Consider the following when hosting a foreign visit:

- Do not allow unannounced foreign visitors access to the facility.
- Do not allow last minute additions or substitutions to a foreign delegation to have access to the facility.
- Verify personal identification against the original visit request when foreign visitors arrive to ensure they are who they say they are.
- Watch for last minute or unexpected changes to the approved visitor roster.
- Ensure there are a sufficient number of escorts to control a visiting delegation.
- Ensure escorts are briefed as to what is critical within the facility (e.g., critical information) and that they know what requires protection.
- Ensure facility employees are briefed as to the scope of the foreign visit and to not discuss anything beyond what is approved.
- If a visitor becomes offended when confronted during a security incident, recognize the confrontation as a collection technique and ask the visitor to leave the facility if he or she cannot abide by the rules.
- Do not permit any cameras or note taking if something in the facility is "sight sensitive."
- Monitor computer access. Workstations should never be left unattended and the computer screen unlocked.

Security Plans and OPSEC Plans

An important countermeasure is the development and use of a security plan (i.e., an OPSEC plan). This plan should address risk and sensitivity factors including security areas, general access areas, activities to be conducted, and material that will be made available to the foreign visitors. A determination of whether sensitive subjects will be shared, and affiliation with sensitive countries or countries identified as state sponsors of terrorism, must be made by the owner/user of the information to be shared. Additionally, any security concerns upper level management has based on sound vulnerability concerns and risk management principles (think the OPSEC review process and OSINT) shall be addressed.

REMEMBER

When interacting with a foreign national visitor, be aware of potential risks before the visit, be alert during the visit, and be cautious in post visit interactions with the visitor. Don't forget that foreign national visitors and assignees are only temporarily associated with your organization. They are still representatives of a foreign government and the information they are given access to must not degrade our national security. By practicing good OPSEC we can ensure our security function will remain productive and vibrant. After all, security is everyone's business.

State of the National Insider Threat Programs

In late December 2021, the Enterprise Threat-Mitigation Directorate (ETD) and National Insider Threat Task Force (NITTF) released the *"State of the Insider Threat Programs: Trends from Annual reports, 2018-2020."* We examined trends from insider threat annual reports received from U.S. Government department and agency (D/A) insider threat programs. The annual reports spanned a three-year period and identified program accomplishments, resources, risks, goals, and challenges. While the D/As vary widely in size and mission, understanding the challenges they share enables us to better advocate for solutions and support to mature and grow the national insider threat community.

A copy of the report can be made available to those with .gov or .mil email addresses.
Please contact NITTF-Assistance@dni.gov to request a copy.

ETD is currently collecting U.S. Government department and agency insider threat 2021 annual reports to produce a follow-on trend report. If your program is willing to share its 2021 insider threat annual report or has any questions about this effort, please contact us at the email address listed above, or reach out to your NITTF/ETD liaison officer.

Now Available: Voices from the SBS Summit Podcast

The Threat Lab

Voices from the SBS Summit is a monthly podcast brought to you by The Threat Lab, the Department of Defense's Counter-Insider Threat Program, and the National Insider Threat Task Force. This monthly series was first released in March of 2021 and features conversations with presenters from The Threat Lab's annual Counter-Insider Threat Social & Behavioral Science Summit. During each episode, Threat Lab team members ask guests for updates to their presentations, including what they didn't have time to talk about, and what's new since last September's Summit. In March 2022, we released the Season 2, Episode 3 where Dr. David Prina and Dr. Kurt Braddock discuss attitudinal inoculation and preventing radicalization, and how this relates to security and workforce protection.

The podcast is available on all major podcast platforms including Google, Spotify, and Apple. To find the podcast on these platforms, search for "Voices from the SBS Summit". To learn more visit: **https://anchor.fm/threatlab**

EPA Insider Threat Program AO Honor Award

Earlier this year, the Environment Protection Agency's (EPA) Insider Threat Program (ITP) received internal accolades in the form of a 2021 Office of the Administrator (AO) Honor Award. Recognition for an AO Honor Award is very competitive and EPA's ITP has demonstrated the highest achievement recognized by the AO.

This cross-agency team collaborated to ensure specialties and expertise were leveraged to develop a proper and fully functional ITP for the EPA. Per Executive Order (EO) 13587, all Executive Branch Departments and Agencies, are required to establish, implement, monitor, and report on the effectiveness of ITPs to protect classified national security information. In FY2021, EPA surpassed a number of major milestones in the development and implementation an agency-wide ITP. This diverse team completed the development of policies and priorities for establishing and integrating security, counterintelligence, user audits and monitoring, and other safeguarding capabilities and practices. The team had to be innovative to achieve its goals in record time by leveraging existing systems and procedures while working remotely due

to the COVID-19 pandemic.

This effort required the background and subject matter expertise of many personnel to weave together a formal ITP while meeting the requirements of EO 13587. Through efforts to develop policies and procedures, information access, user activity monitoring, information integration and awareness training, and systems of record, EPA's ITP team was recognized by the AO. This fast-tracked effort was the result of close coordination, positive intent, and the willingness to collaborate for the good of the Agency and national security.

Please join us in congratulating the personnel working in EPA's Insider Threat Program for the active role they played in achieving this significant accomplishment!

2022 NCITF Interagency Educational CI Series

National Counterintelligence Task Force

The **2022 National Counterintelligence Task Force (NCITF) Interagency Educational CI Series** brings together the diverse perspectives and experiences of NCITF partner agencies in training designed to professionalize and educate the U.S. Government's national security professionals. The Interagency Educational CI series include presentations from Joint Counterintelligence Training Academy, FBI's Counterintelligence Training Center, Air Force Office of Special Investigations, Customs & Border Protection, Department of Commerce, Department of State: Diplomatic Security Service, National Counterintelligence & Security Center, and more.

Topics include a discussion on CI capabilities related to NT-50s, overview of diplomatic privileges and immunities in relation to CI operations, analyzing oral communication and body language in assessing verbal deception, the current CI risk environment, and more!

These monthly sessions are open to all federal agencies and government employees.

For additional registration information, please contact **National Counterintelligence Task Force at FBI_NCITF@FBI.GOV.**

January 2022 ETD Symposium

As a result of the COVID-19 pandemic, continuing education, training, and many other resources for federal government personnel have been on hold, lacking, or complicated by matters like teleworking and cybersecurity concerns. Despite these challenges, the National Counterintelligence and Security Center (NCSC), Enterprise Threat-Mitigation Directorate (ETD) is committed to providing continuous support, products, and a variety of other resources to the federal partner community. From online training courses to monthly virtual engagements, ETD has remained connected with our federal partner community.

One such event was the January 20th, 2022, ETD Symposium, a virtual conference featuring presentations on OPSEC, Insider Threat, Counterintelligence (CI), Supply Chain Resilience, and more. Our guest speakers from the Federal Bureau of Investigation, Department of Homeland Security, Department of Health and Human Services, Department of Energy, Department of Commerce, and NCSC presented to an audience of over 650 security, CI, and insider threat practitioners in the federal partner community. The ETD Symposium connected practitioners directly to various subject matter experts who delivered information valuable to their respective programs. Without the support from our speakers, this event would not have been possible, and we are grateful for their continued patronage and collaboration.

For a listing of next quarter's events, please see the "Upcoming Events" section on page 2.

NCITF NT-50 Security Program

National Counterintelligence Task Force (NCITF)

The NCITF is continuing to support NT-50 agencies through its NT-50 Security Program. The purpose of this program is to provide events, training, information, and guidance to NT-50 agencies who either do not have counterintelligence or national security programs, or who wish to create these programs within their agencies. The NCITF also offers support for NT-50 agencies when agencies identify potential security concerns and need a quick and comprehensive response from the FBI and other federal partners. The NCITF recognizes NT-50 agencies have unique missions which may allow foreign adversaries to target the significant U.S. Government equities held within NT-50 portfolios. NT-50 agency information, even when it is unclassified, is just as important to our nation's health and security as the information held by the intelligence community, and the NT-50 Security Program aims to protect this information through the NCITF's collaborative, interagency environment.

As part of this effort, the NCITF is jointly hosting several upcoming events with NCSC to provide NT-50 agencies direct access to the knowledge and capabilities of the interagency environment. On May 5th, the NCITF's Counterintelligence Educational Series will host a session on successful programs, processes, and capabilities within the NT-50 community. Later in the year, the NCITF will host an NT-50 Panel discussion. This event will include counterintelligence briefings followed by open discussion with a panel of NT-50 security experts.

In support of these efforts, the NCITF will be sending a survey to assess the needs and current capabilities of the NT-50s and their security programs.

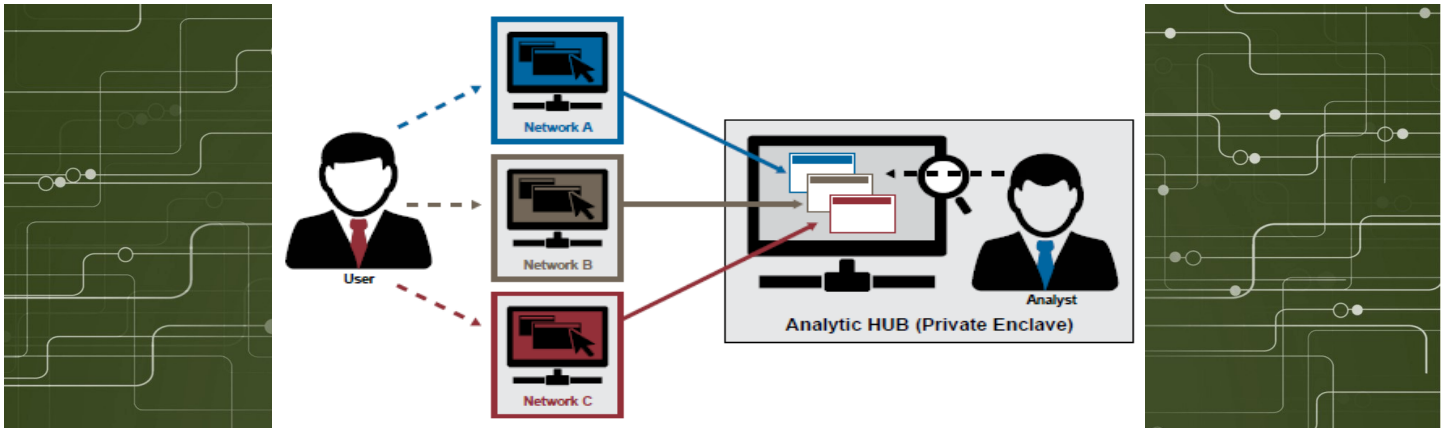
For any questions regarding this program,
Please email FBI_NCITF@fbi.gov or JAMCCRACKEN@fbi.gov.

An Optimum Multi-Network UAM Configuration

In 2014, the Committee on National Security Systems established Directive 504 (CNSSD 504). This technical directive, along with Executive Order (EO) 13587, requires User Activity Monitoring (UAM) to be deployed on all classified networks. Many departments and agencies have also installed UAM on their unclassified networks. Having UAM on each *classified* network fulfills CNSSD 504 requirements, but may not be the most efficient way to track and correlate an individual's anomalous activity.

For instance, if "Jane Doe" has access to Network A, Network B, and Network C, having a UAM capability would allow analysts to track the user's activity on each separate network. However, this inhibits analysts from getting a holistic picture of what Jane Doe is doing across the various networks. Since different analysts may receive Jane Doe's activity alerts, and without the knowledge of the user's activity alerts on other networks, an analyst may view a sole alert as an innocuous event. The ideal solution would be to have Jane Doe's UAM activity correlated from all the networks she has access to and sent to a single UAM server where an analyst can review Jane Doe's activities (i.e.. diagram Network A, Network B, Network C).

An alternative to setting up a standalone UAM network for analysts would be to use a cross-domain solution and push UAM data from other networks to the highest classified network within the agency. This would have the same benefit as having a standalone UAM network where the analyst can monitor Jane Doe's UAM data across all enterprise networks in one central location. The downside to having UAM data stored and analyzed on each enterprise network is that many system administrators will have privileged access to the same networks where their own and their colleagues UAM data is stored. By incorporating a standalone UAM server, the Insider Threat Program can limit the number of system administrators that will have access to the UAM network.



NOTES FROM
THE NOP

January was National OPSEC Awareness Month

This past January, the National OPSEC Program was honored to designate "January" as the official National OPSEC Awareness Month. Since the official designation occurred during the month of January, the NOP encouraged the community and all stakeholders to use the new designation as a formal platform for OPSEC Awareness planning moving forward. The NOP will be planning and collaborating across the community to establish a comprehensive OPSEC Awareness campaign for January 2023. Work is already underway for next year and the NOP will work with the community to ensure a messaging package becomes available this fall for planning and promotion purposes. In the meantime, it was exciting to formally recognize and highlight a month dedicated to OPSEC that our nation could utilize in the vigilant efforts to protect our country.

Working with the OPSEC Community

The NOP and the supporting entities within the ETD continue to collaborate with the OPSEC community to learn more about best practices that are already in place within established OPSEC programs across the USG. Earlier this year, the ETD Client Engagement Group hosted an OPSEC Summit. Deep-dive, round-table discussions provided information on the establishment, development, and maintenance of OPSEC programs throughout the government. The Department of Homeland Security, Social Security Administration, Department of Commerce, and the Department of Defense participated in the summit. The knowledge gained will be shared across the government for other newly established or mature OPSEC programs to use for program development.

Still Need OPSEC Training?

National OPSEC Program resources and training provided by the Interagency OPSEC Support Staff (IOSS) are still available. 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. Virtual instructor-led training, program implementation job aids, computer-based training courses, and other OPSEC-related sessions are available through the IOSS website (https://www.iad.gov/ioss). Register today for training that you need to establish your OPSEC program and/or meet the training needs of your OPSEC practitioners.

The Interagency OPSEC Support Staff (IOSS) currently offers OPSEC training via the following courses; OPSE-1301: OPSEC Fundamentals (self-paced CBT), OPSE-1500: OPSEC & Public Release Decisions, OPSE-2380: OPSEC Analysis, OPSE-2390: Program Management, and OPSE-3500: OPSEC & the Internet. For specific guidance or direction on OPSEC training requirements related to your organization, follow-up with your organization's OPSEC point of contact.

Please note that while the IOSS provides OPSEC training, resources, and services, it DOES NOT establish department, agency, or organization requirements for training or certification levels. The IOSS DOES NOT certify your OPSEC training level. Additionally, the IOSS will provide attendees with a Certificate of Completion for your records and to confirm that the training was completed.

NCSC ETD and the National OPSEC Program office will continue to offer legacy IOSS resources and materials and develop new materials to support federal partner implementation of NSPM-28 requirements.

For more information on OPSEC training, please see page 11.

Insider Risk, Insider Threat Mitigation, & Civil Liberties

Emily Paglicci, NCSC/ETD Virtual Student Federal Service Intern

In government, "insider threat" is generally defined as the likelihood that an individual with authorized access will use that access, wittingly or unwittingly, to do harm to the national security of the United States; and that the threat may be in the form of terrorism, espionage, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities. Capable and effective insider threat programs balance the need to limit the risk posed by those with authorized access against the requirement to uphold each employee, contractor, or affiliate's civil liberties. Ensuring that program procedures and protocols are not only effective, but also address and continue to protect civil liberties for every individual employee, should be a key component of any program.

Civil liberties are defined as basic rights and freedoms guaranteed to individuals as protection from any arbitrary actions or other interference of the government without due process of law. Essentially, they 1) are fundamental rights and freedoms that the Constitution has guaranteed, 2) protect us from overreach by the government, and 3) are unalienable.

When it comes to the intersection of civil liberties and unwitting insider threats, one example to be aware of includes modern medical devices. Many medical devices make it possible for individuals with various physical limitations or medical conditions to fully participate and engage in ordinary work environments. Modern medical devices can include computer chips, Bluetooth, WIFI, microphones, remote control access, data storage, embedded software, and cellular capability. The Americans with Disabilities Act (ADA) along with other privacy and civil liberties laws guarantees staff who need modern medical devices access to the workplace and freedom from discrimination based on their limitations and medical needs. Still, within classified workplaces for example, modern medical devices unfortunately introduce a potential vulnerability exploitable by foreign intelligence services, activists, and criminal groups. Such vulnerabilities include the electronic manipulation of a device to turn it into a listening tool or vehicle for the introduction of malware. It is critical that staff who need medical devices understand their responsibility to report the device(s) to be used to their respective security office, and equally important for security staff, human resources, and other stakeholders to work to find accommodations when necessary.[1]

In the pursuit of identifying malicious insider threat activity and minimizing insider threat risk, it is vital that analytic and investigative activity remain unbiased and nondiscriminatory. Maintaining fundamental fairness in the pursuit of insider risk reduction requires active participation of legal staff during the drafting of policy, creation of standard operating procedures, and implementation of detection tools. Additionally, individuals should never be scrutinized on the basis of national origin, sex, or any other inherent attribute protected by law. For example, in February 2022, Assistant Attorney General Matthew Olsen delivered comments related to espionage, cyber threats, malign influence campaigns, and economic espionage efforts involving China, Russia, Iran, and other nation states, and AAG Olsen noted that it was important to focus on threat activity and not specifically on the nationality or ethnicity of individuals.

The NCSC/ETD and the NITTF have consistently promoted a holistic approach to insider threats, and we continue to encourage organizations to incorporate functions such as human resources, security, legal, and civil liberties to make your programs effective, fair, and innovative. For more information, please see the eLearning course "INT 260.16 Insider Threat Privacy and Civil Liberties" offered by our partner organization, DCSA/CDSE.

[1] In some circumstances, a medical device could also potentially be interfered with due to the nature of the building structure or technology in the workplace, which could jeopardize the health and safety of the employee.

Resource Corner

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

NITTF Website: NITTF would love your feedback as we continue to modify this resource to meet your needs. Be sure to check back for updates.

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

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

Insider Threat Mitigation for U.S. Critical Infrastructure Entities: Guidelines from an Intelligence Perspective.

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.

Insider Threat Sentry **-** Download the free, unclassified mobile application available at Apply App Store and Google Play.

OPSEC 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

10-11 May, 7-8 Jun, 19-20 July, 16-17 Aug, 20-21 Sept

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

12 May, 8 Jun, 21 Jul, 18 Aug, 22 Sept

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

19 Apr, 17-18 May*, 14 Jun, 25-26 Jul*, 23 Aug, 13-14 Sept*

*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 Apr, 24-25 May, 28-29 Jun, 20-21 Jul, 17-18 Aug, 21-22 Sept

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

Senior Official Performing the Duties of the Director of NCSC

Michael J. Orlando

On April 1, NCSC launched the 2022 National Supply Chain Integrity Month awareness campaign, which will focus on securing the information communication and technology (ICT) supply chain. Senior stakeholder commitment, exemplified by the depth and breadth of events scheduled throughout the month, is designed to bring the needed awareness to address software supply chain attack vectors such as the compromise of Microsoft Exchange servers, Log4j software, SolarWinds software, and Pulse Secure products. NCSC is focused on fortifying the ICT supply chain as it underpins government and industry and will further protect US intellectual property, domestic jobs, economic advantage, and military missions. NCSC has developed multiple events, created new resource materials, and updated guidance and best practices to highlight the importance of ICT supply chain security. Please join NCSC by participating in these events or reviewing the supply chain materials on their website NCSC.gov.

"NCSC is focused on fortifying the ICT supply chain as it underpins government and industry and will further protect US intellectual property, domestic jobs, economic advantage, and military missions."

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