October 2021

Volume 1 | Issue 1

ENTERPRISE THREAT MITIGATION NEWSLETTER

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

National Cybersecurity Awareness Month

Robert Rohrer, NITTF Director

Robert W. Rohrer

October is National Cybersecurity Awareness Month. This month we reflect on significant cyber events that have damaged our critical infrastructure, harmed our national security, compromised our personal information and our intellectual capital, and adversely affected our economic base. Recent events, from the ransomware attacks against our energy sector and food supply, to compromises of our intellectual capital and our personal information, highlight the need for us to continue to harden our information systems. National efforts to move towards "Zero Trust Architecture" and "least privilege" (see "NITTF Tech Discussion: Zero Trust & Insider Threat" for definition and additional information) practices are steps in the right direction, making it more difficult for our adversaries to navigate across our systems if they gain access.

As we continue to make progress in countering the technical threats we face, it is important that we also consider the human aspects of the threats. For a decade, the National Insider Threat Task Force (NITTF) and the National Counterintelligence and Security Center (NCSC) have promoted counter-insider threat programs and practices to focus on human behavior within the workforce, contextualize it, and facilitate appropriate organizational responses. We have made great progress as a federal community in building a National Insider Threat Program, and looking at potential human threats from within.

Now, we are asking the community to expand that paradigm. As we look at the external threat we face from our adversaries, we ask you all to view this new paradigm in the same light. It is also a HUMAN threat. Behind the cyber threats we face, there is human intent, capability, and agility. As highlighted in the recent National Counterintelligence Strategy, our adversaries have expanded capabilities and they are using them against a broader set of targets. They use a blended offense, comprised of technical, human, and mixed operations. They migrate across threat vectors in an orchestrated manner, pursuing their strategic objectives.

For years, the NITTF has asked organizations to observe how their workforce behaves. Now, as the NCSC Enterprise Threat-Mitigation Directorate (ETD), we also ask you to look at how the adversary behaves. We encourage you to coordinate all defensive programs in a proactive, orchestrated way - a blended defense to counter the adversaries' blended offences.

INSIDE THIS ISSUE

National Cybersecurity Awarness Month 1

ETD Wants To Hear From You! 2

NITTF Tech Discussion: Zero Trust & Insider Threat 2

SAGE Collaborate Tool 3

FBI's National Counterintelligence Task Force (NCITF) 3

OPSEC: Remember to Remember 4

A Message From the Deputy 5

The New National OPSEC Program Office Set In Motion 7

National Insider Threat Awareness Month (NITAM) 2021 8

Upcoming Events & Resource Corner 8

OPSEC Training 9

Virtual Insider Threat Detection Analysis Course 10

Enterprise Threat Mitigation Seminar Pilot 10

Message From the Acting Director 11

ETD Wants to Hear From You!

The National Counterintelligence and Security Center (NCSC), Enterprise Threat-Mitigation Directorate (ETD) serves as a catalyst for change to improve threat mitigation across the federal enterprise. In order to make improvements, ETD is seeking feedback from its partners across the government. Each year, ETD hosts several Enterprise Threat Discussions, publishes quarterly newsletters, holds forums and conferences, and promotes several awareness campaigns. In order to provide you with information that would be of the greatest benefit to your counterintelligence and security programs, we would like to know your views on:

- **Which topics would you like to see covered by NCSC subject matter experts?**
- **How frequently should ETD host Enterprise Threat Discussions?**
- **How long you would like the Enterprise Threat Discussions to be?**
- **What other recommendations or feedback do you have for ETD's events and products?**

FEEDBACK

Please send your feedback to **NCSC_FEDS@dni.gov**. We look forward to hearing from you and incorporating your recommendations into our future events!

NITTF Tech Discussion: Zero Trust & Insider Threat

Insider threats are on the rise. The reach and consequence of insider threats are increasing due to the sudden growth in telework and cloud migration. Insider operatives often have access to critical data from classified and unclassified systems. The potential unauthorized information they possess can pose a great risk to public and private sectors. To mitigate the growing risk of insider threat activity, many organizations are turning to a Zero Trust model that helps to better modernize security inside and outside the network perimeter with continuous verification of user access.

What exactly is Zero Trust? Zero Trust is a security model that contains a set of system design principles, and a blended cybersecurity and system management strategy based on the understanding that threats exist within and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any single element, service, or node and instead requires continuous verification and validation. The purpose is to ensure that all users and components have the right privileges and attributes to access vital network resources. The principle of least privileged access is one of the core tenets of Zero Trust which means all users should have the absolute minimum permission needed to carry out their work functions and nothing more.

To help protect our Nation's security, on May 12, 2021, the White House issued Presidential Executive Order (EO) 14028. EO 14028 is designed to improve the nation's cybersecurity posture. The EO states that the private sector must adapt to the ever-changing threat environment, and ensure its products are built to operate securely, while partnering with the Federal Government to foster a more secure cyberspace.

The National Institute of Standards and Technology (NIST) is the agency chartered with creating the cybersecurity standards and requirements outlined in EO 14028. Microsoft Inc. and other private and federal partners are working with the National Cybersecurity Center of Excellence to implement a Zero Trust Architecture Project. The project will develop an interoperable approach and design for building a Zero Trust model that aligns with the principles of NIST SP 800-207, Zero Trust Architecture.

Within a Zero Trust security framework, all users go through a strict verification and authentication process. Access is revoked as soon as necessary work is complete and provisioned. Zero Trust presents a shift from a location centric model to a more data centric approach for security controls between users, systems, data, and assets that change over time. This data centric models allows organizations to create policies that provide secure access for users connecting from any device in any location.

Systems that are designed using a Zero Trust model are better positioned to address existing threats and gain greater visibility across the enterprise network landscape. However, Zero Trust implementation is not without its challenges. Zero Trust architecture requires constant maintenance once it is set up. Many different kinds of users, devices, legacy applications, and ways to access data will most certainly present a challenge to the smooth implementation of Zero Trust.

Putting Zero Trust security models into action to proactively manage insider threats helps limit disruptions, strengthens resiliency, and protects users and resources especially in hybrid cloud environments. Zero Trust technologies will help discover risk trends across data, identity, and applications, mitigate risk, and much more.

SAGE Collaboration Tool

The Enterprise Threat Mitigation Directorate (ETD) has acquired the former "ODNI NCSC Federal Partners Group" SAGE (Structured Analytic Gateway for Expertise) collaboration page, now called the "NCSC Federal Partners Page". SAGE was launched in 2011 by the Office of the Director of National Intelligence (ODNI) to support Intelligence Community Directive (ICD) 205 for purposes of leveraging the Federal Government's analytic outreach efforts with outside experts. SAGE is administered by the Defense Intelligence Agency (DIA) and is approved for use of up to the Unclassified//For Official Use Only level information. SAGE provides a secure, unclassified forum enabling collaboration among all levels of government, academia, and diverse private sector industry partners on a plethora of topics. All users are vetted, and access to private pages requires authorization by or invitation from the applicable government space owner.

The ETD SAGE page focuses on sharing information relevant to Federal Government counterintelligence (CI) and security personnel. NCSC newsletters, training, upcoming events, and CI and security related news and information are posted to our page. Moving forward, ETD intends to continue to use SAGE to promulgate insider threat, unauthorized disclosure, OPSEC, and defensive CI information to our colleagues across the government.

In order to increase collaboration and information sharing among CI and security members, ETD encourages CI and security personnel to sign up for a SAGE account in the upcoming weeks. To obtain a SAGE account and join the ETD page, members must have a .gov or .mil email address. To request an account, please email your first and last name, email address, and phone number to NCSC_FEDS@dni.gov.

FBI's National Counterintelligence Task Force

The National Counterintelligence Task Force (NCITF) was established in October 2019 with the vision of uniting the United States Government (USG) to counter foreign intelligence activities. The modern counterintelligence (CI) threat is multifaceted and requires a coordinated whole-of-government approach. The NCITF coordinates these efforts through an interagency task force comprised of approximately fifty (50) member and partner agencies representing the U.S. Intelligence Community, law enforcement agencies, CI components of the U.S. Military departments, and non-Title 50 agencies. NCITF partnerships have resulted in the USG improving its ability to recruit and safeguard sensitive human

sources; facilitated large-scale, multi-agency offensive operations; enabled monthly CI-centric virtual informational series, cyber outreach, and partner engagement; and provided CI training opportunities to partner agencies, particularly those without a traditional CI portfolio.

The NCITF works to coordinate, facilitate, and focus the efforts of the USIC, USG, and the wide array of partner agencies to operate as a single entity in identifying common goals and strategy, prioritizing threats, and standardizing interagency information sharing. If your agency is interested in joining NCITF, please contact **FBI_NCITF@FBI.GOV**.

OPSEC: Remember to Remember

“Not again...Didn’t we just go through Operations Security (OPSEC) training?” If this is your reaction when you receive the annual invite to yet another mandatory security awareness briefing, you have probably been working for the government in one fashion or another for years and could likely give a fairly decent security briefing of your own. Because we deal with sensitive information every day, we might disremember how important that information might be to our adversaries. As experienced and well versed in the security business as we all are, periodic refresher briefings serve to “remind us to remember.”

Take the case of Robert Frederick “Bob” Quick. In 2009, as the Assistant Commissioner of London’s Metropolitan Police Service at New Scotland Yard, Bob Quick was Britain’s senior counterterrorism officer. The position has responsibility for UK counterterrorism as well as protection of the Queen, senior members of the British Royal Family, the Prime Minister, Cabinet Members, and visiting heads of state. At that time Bob Quick had been serving the UK Government for more than 30 years. One can imagine he had received numerous threat briefings and mandatory training. He had likely given a few himself.

So it was a surprise when on 8 April 2009, as Bob Quick exited a vehicle arriving at 10 Downing Street, he was photographed by the press carrying documents marked “Secret.” Not only was the security marking exposed, the whole of the top page was clearly visible and classified details regarding anti-terror “Operation Pathway” were divulged to the press. Additionally, the names of senior officers, sensitive locations and overseas threat information was disclosed. Because of the leak, the MI5 operation to thwart an alleged al-Qaida plot was rushed forward, forcing police to make twelve arrests in daylight and putting the arresting officers in jeopardy.

Luckily no one was injured due to this blunder, but the possibility for a catastrophe or a failed arrest were very real. Prime Minister Gordon Brown’s government and New Scotland Yard suffered great embarrassment. Bob Quick resigned the next day and gave the following statements: “I have today offered my resignation in the knowledge that my action could have compromised a major counterterrorism operation. I deeply regret the disruption caused to colleagues undertaking the operation, and remain grateful for the way in which they adapted quickly and professionally to a revised timescale.”

It’s very possible that Bob Quick was in a great hurry that day and had a lot on his mind. Maybe simple security procedures were so second nature to him that he forgot to remember them. Had Bob Quick adhered to the most basic of OPSEC principles, i.e., knowing what information he wanted to protect and then taking the rudimentary steps to protect it, these humiliations would have been avoided.

Unfortunately Bob Quick is not the only British official who fails to practice OPSEC principles. The photographer who caught this mistake told a news outlet that it is “astonishing” how many ministers and officials continue to enter and exit 10 Downing with sensitive documents on display. He has advised the Downing Street press office a dozen times to say, “For God’s sake tell them to cover up their documents.” Eventually they took heed and posted a reminder at the Downing Street exit to cover all sensitive materials before leaving.

There is no guarantee that Bob Quick’s lapse would have been averted had he received “just one more” OPSEC briefing, but perhaps his example will stick with you and “remind you to remember” OPSEC principles when you have a lot on your mind.

A Message from the Deputy

Rebecca Morgan, NITTF Deputy Director

Rebecca Morgan

In response to significant compromise of classified information and other national security crimes committed by trusted insiders during the first years of the 21st century, President Barack Obama issued Executive Order (EO) 13587 in October 2011. EO 13587 established the National Insider Threat Task Force (NITTF) under joint leadership of the Attorney General and the Director of National Intelligence, headed by the National Counterintelligence and Security Center (NCSC). The new policies directed structural reforms to develop a government wide program for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure. The policy requires federal departments and agencies with access to classified information to establish insider threat detection and prevention programs, and the NITTF to assist agencies in developing and implementing these programs. In November 2012, following an extensive interagency coordination and vetting process, the president issued the National Insider Threat Policy and the Minimum Standards via a Presidential Memorandum.

These policies represented a paradigm shift in U.S. efforts to counter insider threats. While the insider threat was nothing new, and in fact had been with the nation since its founding, most counter insider threat activity was conducted exclusively by security, counterintelligence (CI), or law enforcement entities and focused on incident response rather than prevention. The new policy mandated a proactive, multidisciplinary insider threat mitigation capability that promoted collaboration and information sharing between the traditional elements of law enforcement, CI and security and other discipline areas of cybersecurity, human resources, mental health, and behavioral science. The policy also required collaboration with legal elements to ensure the protection of privacy and civil liberties of the workforce.

> "In the 10 years since the issuance of the Executive Order, the insider threat landscape has changed in unprecedented ways."

Over the last decade, the federal government developed a robust, counter insider threat capability in accordance with policy and minimum standards and moved beyond those standards to a maturity model focused on best practices and incorporating enterprise risk management principles. Investment in training and certification efforts have ensured a professionalized workforce with the knowledge, skills, and ability to implement effective programs. Collaboration with the behavioral science and research community has supported the maturation of the program with best practices and procedures grounded in science and facilitated the ability of federal programs to operationalize research outcomes. Counter insider threat program personnel have matured into an engaged and professionalized workforce committed to sharing best practices and collaborating across the federal government.

While many departments and agency programs are operational and have implemented efforts to mature their insider threat risk mitigation capabilities, in the 10 years since the issuance of the executive order, the insider threat landscape has changed in unprecedented ways. Multiple events have demonstrated that threats posed by trusted insiders are far from static. In fact, the insider threat is a dynamic, ever evolving set of threat vectors ranging from espionage, unauthorized disclosure, fraud, intellectual property theft, mass kinetic violence, and everything in between. Threats posed by insiders present a unique challenge for in the U.S. and worldwide as organizations seek to

mitigate risk while protecting the privacy and civil liberties of the workforce. These challenges are not confined to the components of the Executive Branch. Critical infrastructure sectors, including the defense industrial base and state/local/tribal governments; academic institutions; and private industry from Wall Street to Main Street all face these challenges.

The scope of the insider threat is broad and dynamic. Initial policy under EO 13587 and associated National Minimum Standards were designed to address the many compromises and loss of resources related to high level cases of data leaks which gravely impacted national security. However, the number and type of insider incidents is growing. Over the past 10 years, our Nation has suffered a rising number of incidents perpetrated by trusted insiders that have adversely affected public health and safety, national security, and the economic wellbeing of the U.S. Insider threats include a range of threat actors including cleared and un-cleared federal employees and others with authorized physical or logical access to U.S. Government resources such as vendors, suppliers, and other third parties. The risks associated with trusted insiders have manifested in numerous ways including espionage, unauthorized disclosure, fraud, theft, sabotage, and workplace violence. In the private sector, insider incidents account for billions of lost dollars annually in actual and potential damages related to trade secret theft, loss of proprietary information, fraud, theft, sabotage, damage to an organization's reputation, acts of workplace violence, and more.

Vulnerabilities to risk are increasing. In the decade since initial policy and National Minimum Standards were issued, we have reached a far better understanding of the nature of risk associated with insiders. Initial program requirements were specifically directed to counter technology vulnerabilities from threats posed by insiders. While those technology vulnerabilities continue to exist in both the public and private sector, we acknowledge that as human beings, insiders represent both a potential threat and a vulnerability. Insiders, both witting and unwitting, can cause immeasurable harm to organizations and their resources. They are also vulnerable – to targeting and exploitation by adversaries and to the vagary of stressors of the 21st century environment. From global occurrences such as the COVID-19 Pandemic and climate change, to localized issues such as aging industrial control systems within our nation's critical infrastructure, the risk of insider threat actions are as diverse as the organizations and the workforces that support them. These findings have a fundamental impact on every facet of the insider threat mission and inform the required posture to counter the complexity of the threat in society's professional settings.

Countering insider and adversarial threats requires a sophisticated and coordinated response. Insider threats do not exist in a vacuum. Insiders, whether witting or unwitting, are often a component of adversarial activity against U.S. interests. These activities, including physical attacks, supply chain attacks, cyber-attacks from phishing to ransomware, malign influence, and disinformation campaigns often employ multiple vectors or blended operations. And the human insider is often a component of these operations. In response, we must deploy an enterprise threat mitigation capability to promote active, integrated mission practices that counter all aspects of adversarial and insider threats to public health and safety, economic security, and national security. NCSC advocates an enterprise threat mitigation capability focused on the ***organizational practice*** of actively coordinating defensive capabilities that counter threat actors. This must be a ***leadership driven effort***, distributed across all security domains and organizational programs. We must ***actively*** engage all threat mitigation practices, in a coherent and coordinated manner, to proactively avert harm. We must think beyond traditional security, CI, and insider threat programs and incorporate Operations Security (OPSEC) principals that include all stakeholders in a common mission of countering the risk posed by aggressive threat actors.

The next 10 years poses many challenges to the counter insider threat mission, but the federal insider threat practitioner community has developed into a robust, dynamic, agile workforce well positioned to meet these challenges. NCSC looks forward to championing these efforts as we move ahead together.

The New National OPSEC Program Office Set In Motion

As many of you may have heard, the National OPSEC Program (NOP) and the Interagency OPSEC Support Staff (IOSS), are undergoing a complete transition. With the signing of the Presidential Directive, NSPM-28 in January 2021, the NOP will move and be administered under the National Counterintelligence and Security Center (NCSC). The new organization will become the NOP office and will work within the Enterprise Threat-Mitigation Directorate (ETD) and closely with other mission elements. During this transition, the IOSS will continue some of the OPSEC activities and courses through 2022 until fully transitioned over to NCSC. A timeline for the stand-up of the new NOP office has not been announced.

Various elements of past support are being upgraded and updated to conform to the new look and focus of the NOP and the standards of the NSPM. One of the first products the NOP will be involved in is the Newsletter. Under the new office, we will combine forces with the other mission elements to produce a more comprehensive look at the topics of interest to cater to a larger audience. To assist in this endeavor, the NCSC will be employing a new distribution platform for sending out the newsletter. We will keep the community apprised of our activities through the newsletter. The NOP office is looking forward to the enhanced capability and to the improved communications with the entire community.

As this transition progresses, we will make every attempt to advise you of how the NOP office can and will support the community in its OPSEC related efforts and missions. Change is never easy, but moving forward is always beneficial. We appreciate your patience and looking forward to moving with you.

" The new organization will become the NOP office and will work within the Enterprise Threat-Mitigation Directorate (ETD) and closely with other mission elements."

NITAM
National Insider Threat Awareness Month
SEPTEMBER 2021
#
INSIDER THREAT AND CULTURAL AWARENESS ... #BETHECHANGE

National Insider Threat Awareness Month 2021

The National Counterintelligence and Security Center (NCSC), National Insider Threat Task Force (NITTF) facilitated, conducted, and supported many activities and events leading up to and during the third annual National Insider Threat Awareness Month (NITAM), September 2021. Events and activities conducted during NITAM highlighted the importance of insider threat awareness in preserving our personal safety, economy, and national security and challenged all Americans to help protect, preserve, and strengthen the security of public and private organizations. In addition, it educated government personnel and outside audiences on how to recognize and report potential risk indicators.

In coordination with DoD, NT-50s, and industry partners, NITTF championed NITAM's 2021 theme of providing positive workplace culture to thwart the manifestation of an insider threat that could potentially be fostered in a toxic work environment. Increasing awareness and understanding of workplace cultural differences among employees allows the avoidance of social missteps and unintentional harms. Organizations creating a workplace culture based on respect and understanding and promotion of leadership/organizational loyalty reduces the risk of insider threats.

In case you missed it, NCSC/NITTF's NITAM activities included an endorsement letter from the Acting Director of NCSC to garner insider threat community support to more effectively deter, detect, and mitigate insider threats by increasing awareness and promoting reporting; a special edition newsletter to motivate insider threat programs to raise responsiveness to insider threats; 4 bulletins via NCSC Linkedin account on providing a positive workplace culture and increasing awareness of the insider threat; 4 posters via ODNI digital screens and SharePoint aiming at the ODNI workforce; a kickoff of NITAM via security experts websites/periodicals such as Executivegov.com, FederalNewsNetwork.com, ClearanceJobs.net, CSO Online, Asisonline.org, Security Boulevard.com, & Homeland Security Today; and speaking events at 18 different organizations during August and September to promote insider threat awareness to public and private organizations.

UPCOMING EVENTS

October - *National Cyber Security Awareness Month*
28 October (10am-11am) - Enterprise Threat Discussion - Acting NCSC Director Michael Orlando will discuss defensive CI. Following Mr. Orlando will be a brief discussion on the National OPSEC Program.
November - *Critical Infrastructure Security & Resilience Month*
16 November (10am-11am) - Enterprise Threat Discussion - Zero Trust
7-8 and 9-10 February 2022 - Mobile Training Team (MTT) with SOCOM and JSOC
January - *National OPSEC Awareness Month*

Save the dates coming for -

January (TBD) - Enterprise Threat Mitigation Symposium
March (TBD) - NITTF Senior Official Spring Forum

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.

SAGE Website: See "SAGE Collaboration Tool" on page 3 for details. If you're already a member of the NCSC Federal Partners Page, you can access the page **here**.

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

Cybersecurity Awareness Month (October): Visit CISA's website for the latest updates. The theme for 2021 is 'Do Your Part. #BeCyberSmart'.

Critical Infrastructure Security & Resilience Month (November): Visit CISA's website for more information and additional resources.

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.

OPSEC TRAINING

Establish an account at www.ioss.gov to access the self-paced training or to register for the instructor-led training.

OPSEC Fundamentals (OPSE-1301)

PURPOSE

This self-paced online training is available at www.ioss.gov and provides a basic working knowledge of the five-step operations security (OPSEC) cycle with a focus on its use in the workplace. Upon completing this course, learners will be able to demonstrate their understanding of the OPSEC process and describe how they can contribute to a good OPSEC posture for their organization.

This course is often used as an initial training requirement and/or annual training requirement for the workforce and is a pre-requisite for the IOSS instructor-led training.

OPSEC Analysis Course (OPSE-2380)

PURPOSE

This two-day instructor-led MS Teams course provides learners with training on how to conduct OPSEC analysis. Learners will be able to 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.

This course in recommended for those involved in OPSEC programs e.g., program managers, working group members, coordinators.

WHEN

December 7-8, 2021
January 11-12, 2022
February 8-9, 2022
March 15-16, 2022

OPSEC Program Management Course (OPSE-2390)

PURPOSE

This two-day instructor-led MS Teams course provides learners with the knowledge needed to develop and sustain an effective OPSEC program. Upon completion of the course, 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.

This course is recommended for those involved in OPSEC programs e.g., program managers, working group members, coordinators.

WHEN

December 9, 2021
January 13, 2022
February 10, 2022
March 17, 2022

OPSEC and Public Release Decisions (OPSE-1500)

PURPOSE

This one-day instructor-led MS Teams course addresses the OPSEC issues that should be considered when reviewing information intended for public release and public access. Lessons can be applied to preparing information for release in all forms of media (e.g., print, web postings, and public speeches). After completing this course, the learner 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.

This course is recommended for those involved in OPSEC programs as well those involved in public affairs, marketing, website administration, Freedom of Information Act (FOIA), speechwriting and public speaking, and classification review.

WHEN

October 14, 2021
October 26-27, 2021
November 30, 2021
December 13, 2021
January 19-20, 2022
February 15, 2022
March 9, 2022
March 22-23, 2022

OPSEC and the Course (OPSE-3500)

PURPOSE

This one-day instructor-led MS Teams course introduces OPSEC practitioners to common threats, vulnerabilities, and countermeasures associated with the internet and connected devices. It will assist OPSEC practitioners to better assess the risk associated with the internet.

This course is recommended for those involved in OPSEC programs e.g., program managers, working group members, coordinators.

WHEN

October 6-7. 2021
November 17-18, 2021
December 15-16, 2021
January 25-26, 2022
February 16-17, 2022
March 29-30, 2022

OPSEC for All: Protecting Yourself and Your Critical Information

PURPOSE

This is an editable and modular OPSEC overview developed for OPSEC practitioners who want a briefing that increases the workforce's operations security knowledge and awareness. The PowerPoint slides and fully developed speaker script are unclassified in their entirety; however, based on your situation, you could have discussions that are for official use only or classified. This deck includes a 20-slide OPSEC overview and four standalone five slides modules: OPSEC and Your Family, OPSEC and Your Connected Devices, OPSEC and Work From Home, OPSEC and Social Media. These short modules can be used in conjunction with the overview or independently.

This briefing can be used to fulfill initial training and/or annual training requirements for the workforce.

Virtual Insider Threat Detection Analysis Course

NITTF has partnered with DITMAC and DIA's Joint Military Intelligence Training Center (JMITC) to extend enrollment in the Virtual Insider Threat Detection Analysis course to all Executive Branch departments and agencies at no cost. This course is designed for all federal insider threat program analysts from Department of Defense (DoD), Intelligence Community (IC), and Non-Title 50 (NT-50) communities.

Specifically, this course provides entry level Counter-Insider Threat Analysts the ability to apply critical thinking skills and applicable structured analytic techniques to potential insider threat indicators as learners obtain and use holistic data in conjunction with the application of critical pathway theory. Participants will apply Executive Order, Department of Defense, and IC authorities to gather this holistic data while they ensure constitutional and privacy rights are maintained. Participants will execute the appropriate processes for conducting and reporting insider threat response actions from intake of an initial potential threat to mitigation of the threat. Additionally, participants will be able to disclose mandated counterintelligence and criminal activity information to the appropriate agency/office.

<u>Fiscal Year (FY) 2022 course schedule is as follows:</u>

October 25 to 29, 2021

December 6 to 10, 2021

January 24 to 28, 2022

March 7 to 11, 2022

May 16 to 20, 2022

June 6 to 10, 2022

July 18 to 22, 2022

August 15 to 19, 2022

September 12 to 16, 2022

Please contact Don Parnell at donald.parnell@dodiis.mil or 540-760-5715 to register.

Enterprise Threat Mitigation Seminar Pilot

Enterprise Threat-Mitigation Directorate (ETD) will hold a comprehensive enterprise threat mitigation seminar pilot early second quarter of FY22 in accordance with its new and expanded missions. This seminar integrates the four disciplines of unauthorized disclosures, insider threat, operations security (OPSEC), and defensive counterintelligence to mitigate adversarial and insider threats to national security.

The goal of this seminar is to promote active organizational, integrated mission practices that counter all aspects of adversarial and insider threats to public health and safety, economic security, and national security. Enterprise Threat Mitigation is a leadership driven effort distributed across all security domains and organizational programs. It actively engages all threat mitigation practices, in a coherent and coordinated manner, to proactively avert harm to the United States. Enterprise Threat Mitigation enhances traditional security programs by incorporating OPSEC principals, and including all stakeholders in a common mission of countering the risk posed by aggressive threat actors.

This pilot seminar will be used to refine learning objectives and seminar content with the goal of regular seminar offerings beginning in the latter half of FY22. The target audience for this seminar is NT-50s, DoD, and Intelligence Community Insider Threat Program Managers, OPSEC Program Managers, Defensive Counterintelligence Program Managers, and Senior Security Managers. We look forward to hosting our stakeholders at upcoming iterations of this new offering.

From the Acting Director

Michael J. Orlando
Acting NCSC Director

OPSEC is a disciplined approach to viewing classified or unclassified information and observable activities through the eyes of your adversaries, and implementing appropriate protections and countermeasures. OPSEC is achieved through a process of continual assessment that identifies, analyzes, and addresses critical information vulnerabilities, risks, and threats.

In January 2021, the President signed NSPM-28, which 1) designated the NCSC within the ODNI as the USG lead for OPSEC, 2) expanded the OPSEC scope to whole-of-government and those that do business with the government, and 3) called upon all departments and agencies to partner with state, local, tribal, territorial, and private sector entities to promote use of the OPSEC principals into their operations and activities.

With NCSC leading the NOP Office and incorporating the previous interagency OPSEC Support Staff (IOSS) functions, we are able to enhance OPSEC with a whole-of-nation approach. We are able to leverage national assets and enhance overall training capabilities for OPSEC that may not have been previously available to Federal departments and agencies outside the IC or Department of Defense (DOD) community. This expansion of coverage harnesses the national counterintelligence and security strategies and activities already within NCSC to serve as a fundamental and critical elements to addressing foreign adversarial threats.

> *"NCSC is able to leverage national assets and enhance overall training capabilities for OPSEC that may not have been previously available to Federal departments and agencies outside the IC or DOD community."*

We hope you are finding these Newsletters valuable. If you have any feedback, articles you'd like to submit, or other thoughts on how we can enhance our engagement with the federal workforce, please let us know at NCSC_FEDS@dni.gov. For more information on NCSC CI and security topics, please visit our website at https://www.NCSC.gov or follow us on Twitter @NCSCgov.

Michael J. Orlando