October 2022 Volume 2 | Issue 4

ENTERPRISE THREAT-MITIGATION NEWSLETTER

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

October is Cybersecurity Awareness Month

Robert W. Rohrer
Director, NITTF

National counterintelligence strategic objectives include the protection of American critical infrastructure, our economic base, and our system of democracy. In furtherance of those goals, the National Counterintelligence Strategy calls out the need to defend the American supply chain, and counter adversarial efforts in cyberspace. These objectives articulate what we need to do, or rather what we are defending, and to an extent, where we need to do it. However, as we welcome Cybersecurity Awareness Month in October, we should remember that "cyberspace" in the context of national security is just a place (i.e., a "battlespace"), and cybersecurity is just one element of a larger set of national defense and security practices.

September was National Insider Threat Awareness Month. Last May, we focused on supply chain risk management. In January, we will focus on operations security (OPSEC). This month we focus on cybersecurity. Each of these disciplines has its own mission and needs. All are essential programs for the protection of the cornerstones of American strength: our people, the resources and infrastructure our people use and depend on, and our information (from national security information to our intellectual capital).

Cybersecurity is most often aligned with the protection of information with the goal of "prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."[1] However, like the other disciplines mentioned above, cybersecurity is part of a much broader, and often underrepresented effort: information security or INFOSEC.

There is no National INFOSEC month. As noted, we celebrate pieces of INFOSEC with their own months, but INFOSEC is much broader than any individual program. National Institute of Standards and Technology (NIST) guidance articulates this well, listing OPSEC, personnel security (PERSEC), technical security countermeasures (TSCM), supply chain risk management (SCRM), and even insider threat programs as "controls" toward the goal of protecting information and information systems. INFOSEC is a goal - an endgame.

INSIDE THIS ISSUE

Over the past year, the newly-established Enterprise Threat-Mitigation Directorate of the National Counterintelligence and Security Center (NCSC/ETD) has worked to develop a framework to better coordinate defensive countermeasures, from traditional security programs and defensive counterintelligence efforts, to supply chain and enterprise risk management practices. We have reviewed volumes of U.S. government laws, standards, guidance, policy, and practices. We have looked at formal definitions or noted the lack of formal definitions for the broad spectrum of defensive countermeasures ("defensive counterintelligence" for example has no formal definition), and thrown around the above acronyms we all have come to embrace: OPSEC, PERSEC, SCRM, TSCM, etc.

In the end, we have an enterprise threat-mitigation framework. We took the OPSEC cycle, and laid it over existing federal enterprise risk management practices, and simply put, we are asking our partners to take the foreign adversarial threat (an "advanced persistent threat") into consideration when looking at organization risk, and apply appropriate countermeasures (or "controls").

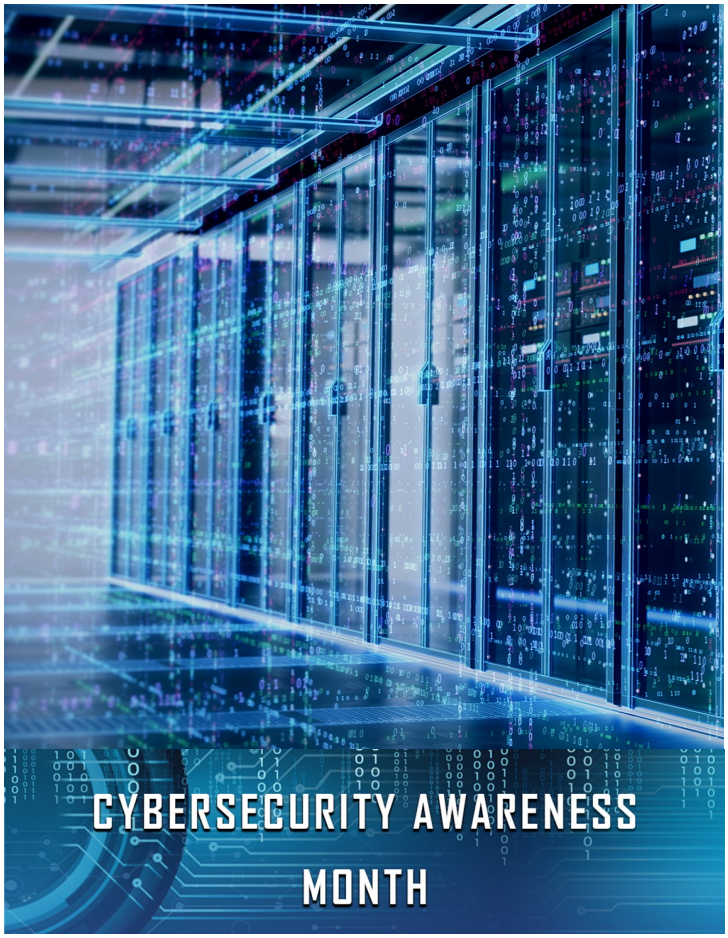
What are we suggesting that is new? What is not already captured in existing policy or requirements? Not much, when you view the effort as INFOSEC practices. OMB Circular 123 asks departments and agencies to adopt enterprise risk management practices. The NIST Risk Management Framework (RMF) provides more detail on how to do that. As noted, numerous NIST Special Publications (in support of the Federal Information Security Modernization Act) provide guidance on protecting information (INFOSEC) as well as information systems (Cybersecurity) through application of "controls" that include OPSEC programs, insider threat programs, personnel security, supply chain risk management, incidents response, and more. They address the protection of controlled unclassified information on government as well as non-government systems, and provide best practices for countering advanced persistent threat. They even address threat intelligence and information sharing.

So what is new? Nothing more than the understanding that foreign adversarial threat is the most advanced and the most persistent of threats, and obtaining our information is as much a strategic goal for adversaries as any territorial claim has been in past conflicts. Cyberspace is only one battlefield in which they are coming after our information, and they are adeptly skilled to utilize any-and-all means to get it. From a risk standpoint (risk = threat x vulnerability x impact), this threat can exploit any vulnerability and create risk where it does not already exist. And the consequences or impact of adversaries achieving their strategic objectives is potentially devastating to our economy, our national security, and even our democratic foundation. With that, the risk we face on an enterprise level across the government and our public and private sector partners is unparalleled in our history.

To counter the risk, our organizations from the top down must understand it and implement appropriate controls to mitigate it where possible. INFOSEC as an organizational practice has never been more important. And there are many federal requirements telling us to do everything we need to do. We just need to do it better - more coordinated and more proactively. We need to understand the threat, where possible attribute the threat to the strategic goals behind it, anticipate the vectors the threat will move across next, and do our best to get ahead of it.

As we welcome National Cybersecurity awareness month, I once again encourage all of our partners across all disciplines to review and renew our broader INFOSEC practices. Look for opportunities to learn more about cybersecurity and how it fits together with OPSEC, SCRM, PERSEC, insider threat, TSCM, and all the other alphabet soup that represents the disciplines we practice. Most importantly, let's remember what it is we are trying to protect this month, and every month.

[1] NIST Special Publication 4009: Glossary of key information security terms



COMMON ACRONYMS

CI - Counterintelligence

D/A - Departments and/or Agency

ETD - Enterprise Threat-Mitigation Directorate

IOSS - Interagency OPSEC Support Staff

NCITF - National Counterintelligence Task Force

NCSC - National Counterintelligence and Security Center

NITTF - National Insider Threat Task Force

NOP - National OPSEC Program

NSPM - National Security Presidential Memorandum

NT-50 - Non-Title 50

OPSEC - Operations Security

UPCOMING EVENTS

October - *National Cyber Security Awareness Month*

November - *Critical Infrastructure Security & Resilience Month*

November 9th - *Insider Threat Program Manager Symposium*

November 10th - *OPSEC Program Status Update Workshop*

January - *National OPSEC Awareness Month*

January 11th - *2nd Annual Enterprise Threat-Mitigation Symposium*

Election Threats Security and Misinformation

Jacob Breach, Partner Engagement, ODNI Election Threats Executive

With the 2022 midterm election cycle in full swing, the United States is confronting persistent foreign threats seeking to influence American public opinion, shape policies, and harm our national dialogue. The Office of the Director of National Intelligence (ODNI) serves as the coordinating authority for the Intelligence Community (IC) on election security and foreign malign influence.

ODNI's Election Threats Executive (ETE) was created in 2019 to coordinate all election security-related activities, initiatives, and programs across the IC. The ETE works across the IC to ensure that our threat information is consistent and clearly communicated to a broad base of customers. ODNI remains focused on adversaries' efforts to try to sway U.S. voter perspectives and preferences, shift U.S. policies, suppress their critics, increase discord, and undermine the American people's confidence in our democratic processes, including elections.

Protecting against these efforts presents a unique challenge. Our election process relies on various physical and cyber assets – such as information technology systems, networks, equipment, and facilities – that are regulated in the United States at the federal, state, and local levels. The IC is also aware that assets comprising the election infrastructure are susceptible to unintentional and intentional threats. Intentional threats can involve targeted and untargeted attacks from a variety of sources, including criminal groups, hackers, foreign nations engaged in espionage and information warfare, and terrorists.

This is also a developing industry. In 2020, the IC tracked a broader array of foreign actors taking steps to influence U.S. elections than in past election cycles. In addition to state actors, public relations, media consulting, and information technology firms are also conducting manipulation campaigns on behalf of a range of foreign clients, forming an emerging market for information manipulation.

In many cases, foreign threat actors focus on exploiting American voices and furthering existing fissures in the U.S. – vice generating new narratives – to try to influence electoral outcomes, increase mistrust in U.S. election processes, and stoke sociopolitical divisions. These efforts are meant to improve the effectiveness of propaganda while providing greater deniability by blurring the line between domestic and foreign-backed content.

Foreign threat actors have demonstrated the ability to tailor content to target audiences across the political spectrum. For example, during the 2020 election, a Krem-

lin-linked influence organization used social media personas, news websites, and U.S. persons to deliver tailored content to subsets of the U.S. population.

Foreign threat actors may target future post-election environments to try to undermine confidence in the integrity of our elections. After the last Presidential election, Iran conducted influence operations to try to inflame domestic tensions in the U.S. and promoted narratives questioning the election results.

These actions from the 2020 election are representative of the kinds of campaigns foreign actors are undertaking to influence the U.S. Government, state and local governments, and the public.

As in many areas, sunshine is the great equalizer for many of these tactics. Greater public awareness of influence operations in 2020 as compared to previous election cycles probably helped counter some operations. U.S. Government public messaging as well as additional government and private sector actions probably also disrupted some activities. For example, proactive information sharing with social media companies facilitated the expeditious review, and in many cases, removal of social media accounts covertly operated by foreign actors.

The threat to U.S. democratic processes and institutions from foreign malign influence is enduring. Informing efforts to counter it requires constant attention, a whole-of-government approach, support from the private sector, and engagement from the public. ODNI is committed to protecting our democratic process and institutions from foreign influence and interference. We thank our interagency partners who are critical to our collective success and look forward to continued partnership and collaboration with all U.S. Government stakeholders.

//

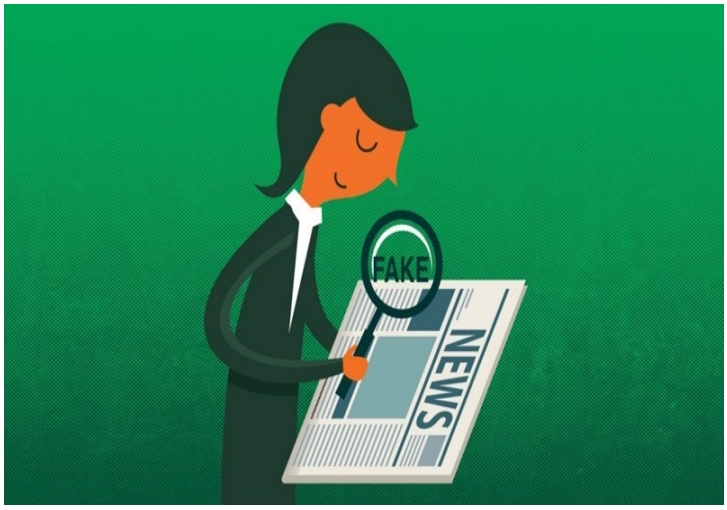
"Foreign threat actors focus on exploiting American voices and furthering existing fissures in the U.S. – vice generating new narratives..."

Let's Be Honest About Mis/Disinformation

Our leaders, politicians, scientists, celebrities, and media figures routinely lecture us about the "threat to our democracy" posed by the information we receive daily through social and other forms of media. Misinformation is generally considered to be information which is inaccurate, but not purposefully so. Disinformation is defined as being intentionally inaccurate for the purpose of influencing recipients. In many regards, the "danger" posed by mis/disinformation is in the eye of the beholder. While conspiracy and unfounded ideas like "replacement" theory[1] are routinely identified as dangerous disinformation, selective mainstream media reporting which warps our sense of the world and its realities is seldom cited as a concern.[2] This failure to recognize and acknowledge the depth and breadth of mis/disinformation in all its forms leads many Americans to question the motivations for the so-called sounding an alarm on the topic. This, in turn, leads to increased levels of distrust among the general population.

Mis/disinformation in all its forms undermines citizens' faith in government and society. Inaccurate portrayals of legislation, judicial decisions, or scientific facts and figures erodes confidence and fosters balkanization based on what are generally termed political beliefs, but which might more accurately be called a propensity to adopt certain world-views. . The willingness of groups of individuals to accept, at face value, information which ranges from one-sided and skewed, to completely fabricated, is indicative of how difficult it is and will remain to get Americans to resist mis/disinformation.

The key factor in developing what some call cognitive immunity, the tendency to resist and be able to identify information that is misleading, distorted, and/or fabricated, is an individual's desire to know what the truth really is. To resist narratives requires a deliberate and con-



sistent utilization of what is termed System 2 thinking. System 2 thinking is the deliberate, slow analysis of information. Unlike the almost reflexive or passive processing of information, the application of critical thinking methods or even just a full and careful read and consideration of words in front of you requires a desire to know the objective truth. It is unfortunate that the increased incidence of narcissism[3], which has been identified in multiple research studies, coupled with increased political polarization and its attending tribalism, make it likely many Americans will reject the strategies and mental exertion necessary to resist mis/disinformation. In fact, many Americans are drawn to the echo chambers which reinforce their pre-conceived notions; intentionally avoiding information and opinions which run counter to their belief system. Increasingly, such echo chambers are not just created on the internet, but are created or enhanced by so called mainstream media sources.[4]

The attitude that my "facts" are right while yours are "wrong" pervades many of the political debates permeating our discourse, and provides opportunities for malign foreign influence campaigns to leverage pre-existing, often ill-informed, positions staked out by major American political parties and lesser-known parties with devoted followers. Russia, China, Iran, and other nation states in addition to terrorist and subversive groups have been able to utilize this phenomenon to exacerbate divides and sow discord among Americans while advancing policy decisions in their favor.[5]

Unless Americans decide they want the real facts and not narrative versions of the truth, mis/disinformation will continue to color public discourse, the forming of our opinions, and decision-making. Failure to identify all forms of mis/disinformation as a serious issue will similarly decrease the likelihood that individuals will see a need to effectively change the way they digest digital and other content. Anytime a group hectors others over their world view, while holding a demonstrably inaccurate view themselves, it is only more likely to exacerbate existing divides.

[1] Replacement theory adherents believe that U.S. leadership, primarily the Federal government is seeking to "replace" the American citizen blue collar work force with cheaper, less skilled, and more dutifully adherent foreign nationals who have entered the country unlawfully.

[2] Research in 2021 by the Manhattan Institute and others has shown that many Americans significantly overestimate the number of minority men killed by police as well as the frequency of violent encounters between police and citizens. Research by a Harvard University Economist, the Washington Post, and FBI annual law enforcement statistics shows that actual numbers are far fewer in frequency and number. Such overestimations are most likely due to the disproportional coverage given to certain types of violence by the news media and within social media.

[3] McCain, J. L., & Campbell, W. K. (2018). Narcissism and social media use: A meta-analytic review. Psychology of Popular Media Culture, 7(3), 308. As reported by the Newport Institute of Mental Health

[4] Pew Research Center study published in July 2022 shows that while the majority of Americans (76%) want equal news coverage of both sides of an issue, more than half of U.S. journalists (55%) believe that all sides of an issue do not deserve coverage.

[5] Both the former commander of NATO forces and former Secretary of State Hillary Clinton have revealed that Russia has leveraged the environmental movement to push false information regarding such topics as fracking and fossil fuels. Analysis by internet security company, Mandiant, has shown that a Chinese disinformation group labeled Dragonbridge has sought to use social media to undermine Western companies which mine and process rare minerals in an effort to monopolize the harvesting of raw materials necessary for sophisticated batteries, computer chips, and military applications.

The Risks of Online Professional Networking

Are you looking for a new job, or trying to expand your professional network? If so, chances are pretty good that you're leveraging an online professional networking tool or resume database. These can be incredibly useful, and sometimes necessary, but it's important to recognize potential risks so you can protect yourself as well as your employers and clients from adversaries!

The Defense Counterintelligence and Security Agency hosted a webinar, "Mitigating Threats from State Actors on LinkedIn" on 07/21/2022; LinkedIn representatives stated nation state activity is one of the primary threat vectors they see on their site. The most common nation state activities are human intelligence, malware, and malign influence campaigns.

This activity has played out in court cases, including the case of Jun Wei Yeo, who was sentenced to 14 months in prison after pleading guilty to one count of not registering as an agent of a foreign power in 2020. Yeo, a Singaporean national, worked under the direction and control of the People's Republic of China (PRC) Chinese Intelligence Service (PRCIS). His Statement of Offense details how he used online social networking and media sites (including setting up a fake consulting company and job postings) to spot and assess U.S. persons with access to valuable information. Yeo built a rapport and identified individuals who had financial stress and were not happy at work, and then invited them to write reports and paid them for their work.

In 2019, Kevin Mallory was sentenced to 20 years in prison and five years of supervised release after being convicted for conspiracy to transmit national defense information to an agent of the PRC. Mallory was recruited via a professional networking site and inspired a short film, The Nevernight Connection, by the Federal Bureau of Investigation and the NCSC.

There isn't any evidence the threat is decreasing, so how can you strengthen your defenses and mitigate risk?

- Think critically about the information you include in your resume and how much you talk about your work. Don't post or share anything sensitive or classified and ensure you follow your organization's policies regarding pre-publication or security review.
- Be skeptical when someone reaches out to connect, and learn ways to identify spam, phishing and scams, and fake profiles. Only accept invitations from people you personally know and validate the request if possible.
- If an offer seems too good to be true, it probably is (e.g., someone paying for you to attend or speak at an international conference).
- Double check your security and privacy settings. Use two-factor authentication, hide your personal contact information, and limit the visibility of your profile.
- If you work in human resources (HR) or recruiting, consider regularly checking to see if profiles claiming to be associated with your organization are accurate. An adversary could be trying to make themselves look like a legitimate fellow HR professional or recruiter.
- Report fake profiles to the host. In LinkedIn, if someone sent you a direct message, you can report from the conversation without the need to click on the profile.
- Report suspicious approaches to your security office.
- Build personal resilience so you're better able to respond to stressful life events and overcome adversity.

"LinkedIn representatives stated nation state activity is one of the primary threat vectors they see on their site. The most common nation state activities are HUMINT, malware, and influence. "

2023 Federal Counter Insider Threat Community Recognition Program

If you joined the ETD Discussion last month, you heard about the 2023 Federal Counter Insider Threat Community Recognition Program! We had a robust response last year and look forward to hearing about all the great contributions you made to the community in 2022. This annual non-monetary, honorary recognition program allows federal counter insider threat practitioners to identify and nominate peers in recognition of significant contributions to the counter insider threat mission by executive branch department and/or agency (D/A) insider threat programs and associated personnel. The NITTF, OUSD(I&S), and DHS encourage individuals and teams to submit nominations in the following categories:

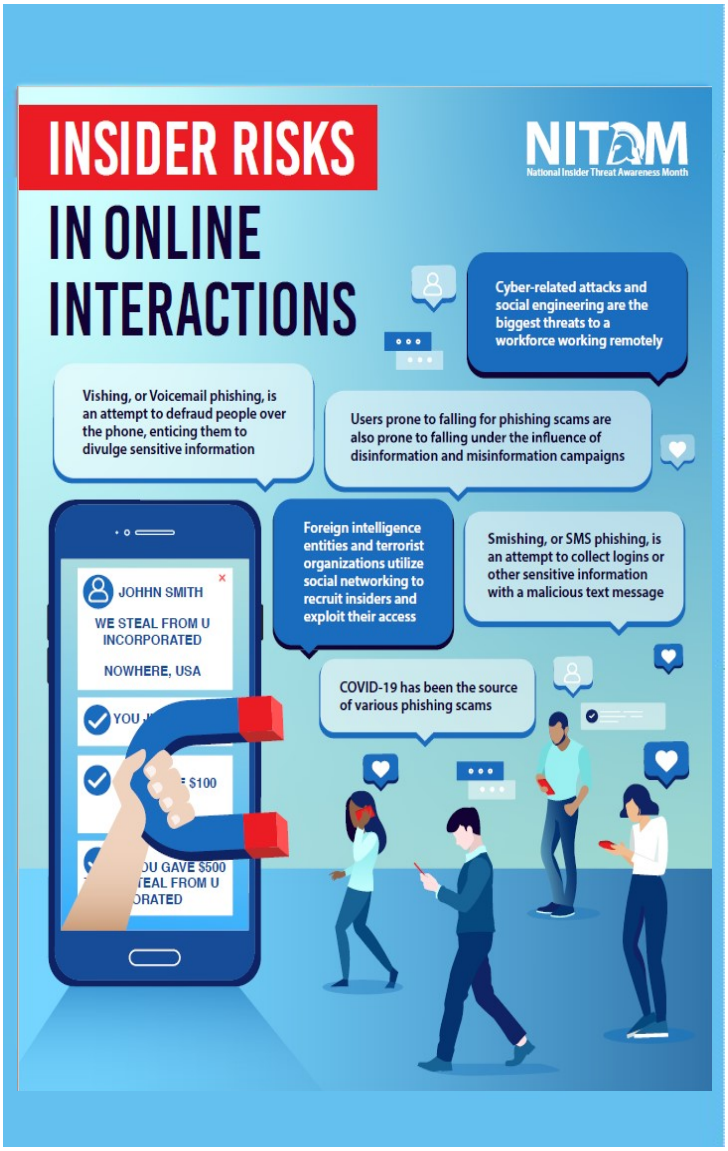
- Closing Gaps
- Detection and Mitigation
- Engagement and Collaboration
- Training and Awareness

The nomination period will be open December 1st, 2022 to February 28th, 2023. Please contact Caren Roushkolb at carenmr@dni.gov or Betsy York at betsyy@dni.gov if you have any questions or need the submission guide and forms.

National Insider Threat Awareness Month 2022

Last month, the NCSC and the National Insider Threat Task Force (NITTF) supported and facilitated several activities for the fourth annual National Insider Threat Awareness Month (NITAM). NITAM is an annual, month-long campaign held during September to educate government and industry about the risks posed by insider threats and the role of insider threat programs. This year's theme, "Critical Thinking in Digital Spaces", highlighted the importance of critical thinking to help workforces guard against risk online, which can facilitate insider threat activity. Such risk includes social engineering efforts; online solicitation by foreign or domestic threats; misinformation, disinformation, and mal-information; as well as malicious cyber tactics like phishing, smishing, and vishing.

The NITTF is currently housed within NCSC. Since its inception, the NITTF has worked with federal departments and agencies to build programs that deter, detect, and mitigate insider threats. NITTF and NCSC coordinate insider threat training and awareness; liaison and assistance; governance and advocacy; and research and analysis for stakeholders in the public and private sector to reduce the risk of insider threats to public health and safety, economic security, and national security. This year, NCSC and NITTF supported several NITAM activities, to include: an endorsement letter from the Senior Official Performing the Duties of the Director of NCSC, Michael Orlando; several posts to NCSC's official Twitter and LinkedIn pages; five bulletins were shared with stakeholders each week and posted to NCSC's website and social media; and speaking events at 16 different organizations to promote insider threat awareness to public and private sector organizations. We hope you were able to join us for one of these events and encourage you to continue sharing our NITAM products with your colleagues throughout the year.



Case Study: ODNI Introduces New Talent Exchange Program With Private Sector

Jessica Hrabosky, ODNI Office of Strategic Communications, and Kevin Krueger, ODNI IC PPTE Program Manager

It is not cliché to say that U.S. Government processes and programs evolve every year and that any new process and/or program can potentially increase counterintelligence and security risks and threats. The ODNI Intelligence Community (IC) Human Capital Office recently established an IC-wide Public Private Talent Exchange (PPTE) program, based upon 50 USC § 3334, that enables IC elements to partner with private-sector companies for additional opportunities. Many of our readers could be impacted by this new program due to potential insider threat and OPSEC equities, and for those that aren't directly affected by this specific program, it may be prudent to determine whether your department or agency has similar programs and how those programs affect your CI and security posture. For those of you who are not familiar with the program, we will give a brief summary then discuss its CI and security implications.

On May 7, 2022, the Director of National Intelligence signed an Intelligence Community Policy Memorandum establishing the IC PPTE. IC elements can now leverage the policy to send their officers to the private sector while the IC can now host private sector staff. The program design provides flexibility for the IC and private sector to partner with each other and share knowledge, best practices, and lessons learned about mission focus areas critical to our national security.

The IC PPTE program management office, housed in the IC Human Capital Office's Workforce Shaping Group, oversees and facilitates the program. ODNI launched the IC PPTE program publicly during a virtual Industry Day event in late June 2022. The program is a great opportunity to get a different perspective on the IC not only from outside the IC, but outside the government. We also hear a lot about industry best practices, culture,

"Many of our readers could be impacted by this new program due to potential insider threat and OPSEC equities... it may be prudent to determine whether your department or agency has similar programs and how those programs affect your CI and security posture."

innovation, etc., and this is a way to experience that first hand - to understand how other organizations approach what they do and to bring that perspective back to ODNI.

The initial program launch includes pilots focused on certain critical focus areas, with each being unique when considering whether to send IC officers out to private sector entities, requesting industry experts to join the IC on an assignment, and in some cases opening the opportunity to both directions. The pilots focus on Data Management, Artificial Intelligence/Machine Learning, Economic Security and Financial Intelligence, Space, and Human Capital.

IC PPTE assignments are contingent on signed agreements by all parties, and other requirements. Assignments vary between 3 months and 2 years and individuals are paid by their employing organization. IC officers will be able to find IC PPTE assignment opportunities in the Joint Duty Application Tool.

"Whether it be technology, innovation, or expertise, among others, industry plays a key role in our national security and for the IC in particular," said Assistant Director of the National Intelligence for Policy and Capabilities Dustin Gard-Weiss. "We need to continue to explore ways for government and industry to partner and work together, to strengthen this important relationship."

From a CI and security perspective, insider threat and OPSEC personnel should ensure that policies and procedures are applied to these programs in order to negate risks. Best practices would include actions such as ensuring that personnel from outside your D/A are appropriately vetted and trained with regard to insider threat and/or OPSEC, and that all relevant disclosure forms are signed. Section B.12.g of the DNI's IC PPTE Memorandum also notes that "any private sector detailee receives the appropriate level of security clearance and eligibility for access to classified national intelligence during the period of the detail assignment, in accordance with applicable laws and policies, prior to the onset of the detail."

CI and security personnel should also be aware that personnel from outside a D/A are most likely not accustomed to your D/A's culture. If that's the case, incoming industry experts may need training or orientation related to these types of cultural issues. Lastly, because these experts have entered into an agreement with your D/A, you will want to ensure that your insider threat and OPSEC operations are minimally impacted and that D/A stakeholders such as civil liberties, human resources, general counsel, etc. continue to be aware of ongoing insider threat or OPSEC risks with these programs just as they would be with other D/A programs.

For more information about the IC PPTE program, contact the IC PPTE program office at IC_PPTE@odni.gov or (301) 243-0366.

2022 National Intelligence Professional Awards

On Thursday, 11 August 2022, NCSC hosted the 2022 Intelligence Community National Counterintelligence and Security Professional Award ceremony. The awards are presented on an annual basis to CI, Security, or other professionals for contributions to the CI and security mission that most significantly benefitted the IC or national security. Awardees from all over the world, including Turkey, Germany, and Hawaii, participated in this year's ceremony. The speakers for the ceremony included the keynote speaker, Principal Deputy Director of National Intelligence Dr. Stacy Dixon, as well as the NCSC Deputy Director, Michael Orlando, and Masters of Ceremony Ms. Olga Delgado and Phil Mountjoy. The audience included officers from the Intelligence Community and Services (Army and Air Force), heads of agencies, Awards Review Board members, NCSC Assistant Directors, and Awards Planning Committee members.

This year's awards program received 76 nomination packages from elements all across the Intelligence Community. Organizations with personnel selected to receive these awards included AFOSI, Army, CIA, DIA, Department of Defense, Department of Justice, Department of State, ODNI, DCSA, FBI, NCIS, NGA, NRO, NSA, and the USAF. This year we recognized 14 teams and nine individuals for CI and security excellence, plus one team and one individual for the Director's Award for Excellence.

NCSC recognizes that it is more important than ever to honor the individuals and teams from across the Intelligence Community for their incredible work defending our nation, and for keeping the American people safe through extraordinary counterintelligence and security work.

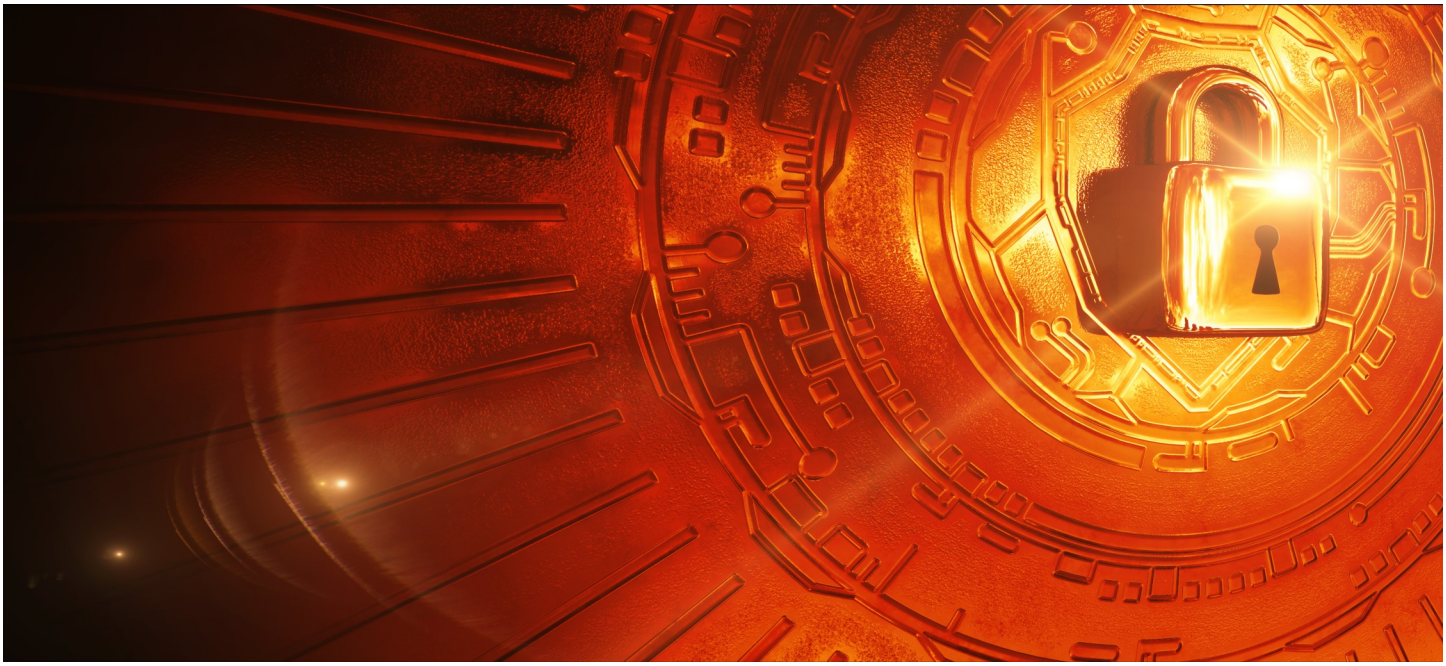
Planning for next year's award ceremony is already underway. Please note that nominations for the 2023 National Counterintelligence and Security Professional Awards are due February 07, 2023.

Coming Soon: 2022 National Intelligence Strategy (NIS)

The 2022 National Intelligence Strategy (NIS) is due to be released in the next few months. Development of the NIS started in spring of 2021 with a fundamental review of the last NIS. Development of the strategic arc, goals, and objectives have been shaped by the 2021 Interim National Security Strategic Guidance, DNI priorities and principles, and the emerging strategic environment that the IC must understand and navigate. The ETD Newsletter staff wanted to ensure that insider threat and OPSEC professionals were aware that the document was on its way and the impact the NIS will have on our organizations and missions. We thought it would be helpful to answer a few frequently asked questions about the NIS...

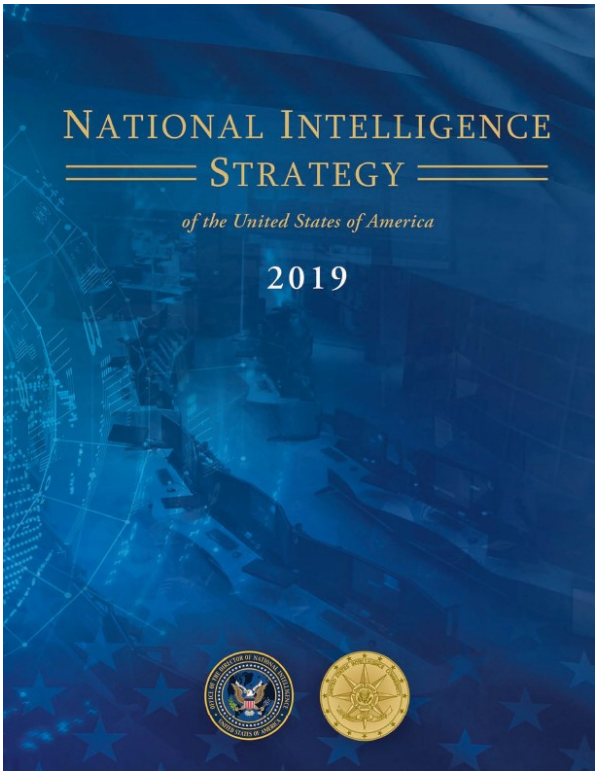
I'm not in the Intelligence Community (IC). Why should I care?

The NIS provides strategic direction for the IC for the next four years and beyond. It also sets the mission and vision of the IC. It articulates the IC's role in supporting the National Security Strategy goals put forth by the President. The NIS serves to align IC activities with Presidential direction, national security, and DNI priorities. While the NIS is intended to provide strategic direction to the IC, it is also intended for a wider audience. One of two unclassified documents issued by the DNI, it does impact those parts of the U.S. Government, governments at every level within the U.S. (e.g. state, local, etc.), IC partners, private sector companies, and individual U.S. citizens who have an interest and a stake in national security matters.



Who creates the NIS?

Four National Intelligence Strategies have been released to date: 2005 (Director John Negroponte), 2009 (Director Dennis Blair), 2014 (Director James Clapper), and 2019 (Director Dan Coats). The 2015 Intelligence Authorization Act requires: "Beginning in 2017, and once every 4 years thereafter, the Director of National Intelligence shall develop a comprehensive national intelligence strategy to meet national security objectives for the following 4-year period, or a longer period if appropriate." At the direction of the Director of National Intelligence (DNI), the NIS is written by a team of strategic planners within the Office of the Director of National Intelligence's (ODNI) staff, in collaboration with subject matter experts from across the IC and Executive Branch of the U.S. Government. Per 50 U.S. Code § 3043a, the NIS is informed by the National Security Strategy, the strategic plans of other relevant departments and agencies of the United States, and other relevant national-level plans. The NIS is coordinated across the IC, reviewed, and signed by the DNI before its release.



When does the new NIS take effect?

The new NIS is effective upon signature by the DNI. Once signed, the NIS will be promulgated by ODNI staff through multiple media sources, and will be posted to the unclassified ODNI website at www.odni.gov. For those interested in reading the current NIS (NIS 2019), you can find the document at https://www.odni.gov/index.php/newsroom/reports-publications/reports-publications-2019?start=5.

Internet Safety and OPSEC

Many of us know the definition of a malicious insider who makes a conscious effort to defraud, steal, and/or leak proprietary information from a public/private institution or government agency. An unwitting insider threat can cause just as much damage and potentially leak even more information than that of a malicious insider. Being an unwitting insider threat to your organization can happen in various forms, to include poor OPSEC. Below are a few scenarios explaining how a person can become an unwitting insider threat through just a few innocuous missteps.

One thing everyone can do to diminish their chances of becoming an unwitting insider threat is to familiarize themselves with the OPSEC Cycle (Identify Critical Information; Analyze Threat; Analyze Vulnerabilities; Assess Risk; Apply Countermeasures; Periodic Assessment). Understanding your position within your organization and who the potential adversaries may be will assist you in being more cognizant of how you can be manipulated and/or tricked into becoming an unwitting insider threat. One step in the OPSEC cycle is understanding your organization's critical information. Once you identify your organizations critical information and recognize who would benefit from having unauthorized access to it, you can then begin taking steps to protect yourself, the information, and your organization.

After identifying your organization's critical information, the next step is to analyze threats, which can be foreign intelligence entities (FIEs), domestic organizations, trusted insiders, and others. Analyzing your vulnerabilities is next. Due to the recent pandemic, many organizations have turned to teleworking to allow personnel the ability to continue working. As you can imagine, teleworking increases vulnerabilities of your data. To minimize this risk, organizations should have a solid teleworking plan and establish a security posture for teleworking devices. Allowing friends/family members to use your teleworking devices to check email, play online games, do school work, etc., can potentially introduce malware, viruses, and other malicious threats. Teleworking also introduces other vulnerabilities because your home network has several other devices that are connected to the Internet. It only takes one connected device to infect your home network which can then infect your teleworking device and potentially infect your organization's network.

Social media and online gaming are other areas where you can potentially be exploited and become an unwitting insider threat. Social media posts can give an adversary pieces of information about you and your organization. Online gaming provides adversaries the opportunity to befriend prospective insiders and over time gain tidbits of information that can lead to an organization being exploited.

Applying countermeasures is another component of the OPSEC Cycle. Some countermeasures that can be implemented are providing timely software updates, adjusting settings on apps to limit who and what has access to your account information, and implementing data encryption. OPSEC countermeasures mitigate risk by reducing the probability of an adversary observing indicators or exploiting vulnerabilities. To learn more about OPSEC and Internet safety you can sign up for NCSC's OPSEC 3500: OPSEC and the Internet course via the IOSS website (www.iad.gov/ioss).

Counter-Insider Threat Research & Practice Annual

The Defense Personnel and Security Research Center's Threat Lab and The National Insider Threat Task Force are proud to announce the publication of the inaugural issue of Counter-Insider Threat Research & Practice (CITRAP). CITRAP is a peer-reviewed, unclassified, open-access journal, serving as an interdisciplinary and multidisciplinary resource for scholarly works across a broad spectrum of the research and operational communities. These communities include the computational sciences, behavioral sciences, public policy, law, and industry.

The inaugural issue contains two original research articles, three "scholarship in practice" articles, and three "perspectives" articles by thought leaders and stakeholders. Visit Counter-Insider Threat Research and Practice (scholasticahq.com).

OPSEC Community Updates from the NOP

2022 has been a big year for OPSEC! Below are two impactful items for the OPSEC community!

OPSEC PROGRAM GUIDANCE AND SUPPORT

The ETD and the NOP have worked diligently to craft guidance and support for the OPSEC community as you develop new OPSEC-related programs to meet NSPM-28 requirements. We knew it would be a heavy lift for many organizations that did not have an OPSEC program in place, or for organizations that face challenges with improving or expanding their current OPSEC programs based on the updated requirements. In June, the National Security Council (NSC) established key OPSEC program requirements for departments and agencies, with a program status update due to the NOP by December 31, 2022. As a result, the NOP developed a robust package of supporting documents, guidance, and implementation goals to fall in line with NSC's requirements. This package was sent to all departments and agencies in July 2022. In addition, with the understanding that building an OPSEC program from the ground up or growing an existing one would have its challenges, the NOP and ETD scheduled two OPSEC Progress Report Workshops to aid and support the community. These workshops provided a deep dive into the OPSEC program and assessment overviews, a review of the OPSEC assessment checklist, and panel discussions with OPSEC experts who shared their knowledge and experience with participants. The goal? To set everyone up for success! The NOP and ETD will continue to adapt, support the entire OPSEC community, and assist with training and guidance for anyone who needs it!

NATIONAL OPSEC AWARENESS MONTH

January 2023 marks the 2nd annual National OPSEC Awareness Month! As we approach the end of 2022, we encourage the community to start or continue to get the word out and plan for this national month of OPSEC! This upcoming year will be the 2nd year to recognize, educate, and celebrate OPSEC on a national level! The NOP is here to support the efforts of community's awareness campaigns, planned events, and continual growth of their OPSEC programs. Please visit the "Operations Security" webpage on the NCSC.gov website for additional OPSEC resources, training, and information!

OPSEC TRAINING

NOP friendly reminder...In order to prepare your OPSEC program for the upcoming assessments, you and/or your team may want to hone your knowledge or skills by getting a little training. OPSEC courses are still available through the end of 2022! The OPSEC courses (see next page) are virtual and easy to access via MS Teams. Don't wait, schedule your courses today!

Critical Thinking and Mis-, Dis-, and Malinformation

The Threat Lab, PERSEREC

The information landscape is more polluted now than ever. The use of mis-, dis-, and malinformation (MDM) can manipulate public opinion and undermine our trust in institutions. Regardless of intent and motivation, the impact of each of these can be equally damaging, particularly because these types of information can spread quickly and are often compelling, evoking emotion.

Building our cognitive immunity allows us to 1) make inferences and draw conclusions based on the evidence presented, 2) assess the potential for misleading information, and 3) better identify false information. We can strengthen cognitive immunity on several fronts by improving critical thinking and media literacy and building awareness of how MDM exploits cognitive biases.

Security professionals should be aware of how MDM can threaten their organizations. Strengthening their people's analytic capabilities helps develop resistance to MDM and develop cognitive immunity.

This article from The Threat Lab defines MDM and explores the benefits of critical thinking. It provides practical ways to challenge cognitive biases and defend against social engineering and phishing. Learn more about these different techniques to analyze and evaluate information as a critical defense.

Training and Education

OPSEC Training

All courses are instructor-led via Microsoft Teams. For more information, or to register, visit the NCSC OPSEC webpage at the following link: NCSC OPSEC webpage. Please note: At this time, the courses below are only open to federal employees, U.S. military personnel, and federal contractors.

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
15-16 November, 13-14 December

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
17 November, 15 December

For future training opportunities, please click on the NCSC OPSEC webpage link listed at the top of the page. The website will be updated as new training classes are scheduled.

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
1-2 November*, 6 December

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
16-17 November, 14-15 December

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

Senior Official Performing the Duties of the Director of NCSC

Michael J. Orlando

National Insider Threat Awareness Month (NITAM) has been a consistent success for agencies across the federal government and our partners in industry. This year was no different as NCSC's National Insider Threat Task Force (NITTF) collaborated closely with the Office of the Under Secretary of Defense Intelligence and Security, the Defense Counterintelligence and Security Agency, and the Department of Homeland Security on this important initiative.

I particularly liked this year's NITAM campaign focus, which highlighted the importance of critical thinking to help our workforces guard against risk in digital spaces. In the IC we use critical thinking skills routinely. Encouraging workforces across government and industry to analyze and effectively break down issues to make better digital decisions makes perfect sense. Critical thinking skills are essential to reduce vulnerability to growing risks in both the physical and digital workplaces of today.

> *"Critical thinking skills are essential to reduce vulnerability to growing risks in both the physical and digital workplaces of today."*

I was fortunate to participate directly in several NITAM events during September and was able to see firsthand the level of effort sustained during the month and the dedication of everyone involved in raising awareness and delivering our joint messages regarding insider threats. Thanks to all of you who participated in NITAM activities for your role in this effort.

I know this same commitment will be applied as we prepare for January 2023 and OPSEC Awareness Month. National Security Presidential Memorandum (NSPM) 28, designates NCSC as the U. S. Government lead for operations security. ETD personnel work tirelessly to promote partnerships between federal agencies and State, Local, Tribal and Territorial government entities and the private sector. Our adversaries also work tirelessly as they seek to gain information from us and our partners. Keeping information safe is vital and requires diligence and constant awareness to be successful. OPSEC Awareness Month actively promotes these positive behaviors.

I 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