JANUARY 2023 VOLUME 3 | ISSUE 1

ENTERPRISE THREAT-MITIGATION NEWSLETTER

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

CELEBRATING OUR COMMUNITY SUCCESS

Rebecca Morgan
Acting Director
ENTERPRISE THREAT-MITIGATION DIRECTORATE

Happy 2023 to the NCSC Enterprise Threat Mitigation Community!

We are so grateful for the partnership and look forward to another year of collaborating with each of you. As you know, January is **National Operations Security Awareness Month**. It provides an excellent opportunity to share awareness materials and promote good OPSEC practices throughout your organization. The NCSC National OPSEC Program Office has developed a robust selection of resources to support your organization's participation in the campaign this month and throughout the year. There are many ways to get involved, and efforts both large and small can have a big impact on the security posture of your organization. We'd love to learn more about your OPSEC Awareness activities so please reach out and let us know how it went at your organization.

As members of the national security community supporting OPSEC, Insider Threat, Cybersecurity, INFOSEC, Defensive Counterintelligence, or other critical security programs, you are aware of the heightened risk environment. Throughout this newsletter you'll find reference to real world threats that have impacted our partners in both the public and private sector. Each of these examples highlights the need for holistic enterprise risk mitigation strategies to counter the sophisticated, and often blended, operations of our adversaries. Both OPSEC and Insider Threat embrace a multidisciplinary approach to deter, detect, and mitigate risk. NCSC/Enterprise Threat-Mitigation Directorate (ETD), through both the National OPESC Program Office and the National Insider Threat Task Force (NITTF), encourages practitioners in both mission areas to work with each other and other stakeholders in your organization to develop and implement effective programs.

On a personal note, my Joint Duty Assignment with NCSC is coming to a close. After nearly two decades of working with the NCIX, NCSC, and NITTF, it has been an absolute pleasure to serve with the team. Despite organizational changes and a challenging threat environment, NCSC/ETD accomplished so much over the last few years. It has been one of the best experiences of my career to work with these dedicated

WHAT'S INSIDE

individuals. To paraphrase Winston Churchill – never before have so few given so much for so many. Just a few highlights:

NCSC/ETD has increased engagement with our stakeholders to include monthly Enterprise Threat Discussions, quarterly newsletters, increased training and tabletop exercise opportunities, and robust communications and resources in support of Insider Threat and OPSEC Awareness Months. We also took on the role of executing ODNI responsibilities under ICD 701 for unauthorized disclosures within the Intelligence Community (IC).

> NCSC/ETD, through both the National OPSEC Program and the NITTF, encourages practitioners in both mission areas to work with each other and other stakeholders in your organization to develop and implement effective programs.

The NITTF continued to serve as the mission manager for the National Insider Threat Program, and to support program implementation and maturation throughout the community. More than a dozen departments and agencies achieved FOC and/or demonstrated alternately effective, mature programs. The NITTF also:

- Issued directives and advisories to support training requirements, program maturation, and resourcing, and the implementation of Trusted Workforce 2.0.
- Collaborated with OUSD (I&S) on the Counter Insider Threat Professional Certification as it achieved accreditation and piloted a Global Certification that is set to become the new standard.
- Continued support to the Insider Threat Legal Working Group (WG), NARA Records Retention WG, and other initiatives to overcome implementation challenges.
- Introduced the Federal Counter Insider Threat Recognition Program to highlight the amazing efforts of the community, and published analytic products to share the state of the federal insider threat program.
- Funded and oversaw significant social and behavioral analytic research with our partners at PERSEREC Threat Lab, resulting in more than 40 new resources including training sessions, performance support tools, and events.
- Advocated for our federal partners before the National Security Council, pursuing policy updates and resourcing to position the federal government to mitigate insider risk in the years to come.

In this short time, NCSC/ETD also stood up the National OPSEC Program Office. By leveraging the expertise and resources from the NSA Interagency OPSEC Support Staff (IOSS), we were able to provide seamless support to the OPSEC community as that program sunsetted. Since its inception, the Office has –

- Trained more than 2,000 students per year, issued National OPSEC Training Standards, and developed job aids and other performance support tools.
- Successfully petitioned to adjust NSPM-28 dissemination markings, and provided guidance and workshops to support OPSEC Program Status Update requirements.
- Advocated on behalf of executive branch departments and agencies before the National Security Council to devise a realistic implementation plan, and articulate the need to fully resource organizations.
- Implemented a National OPSEC Awareness Month and championed OPSEC best practices throughout the community.

NCSC/ETD has increased engagement across the US Government and with external partners, bringing the missions of Insider Threat and OPSEC on par with the other mission areas within NCSC. We have engaged with hundreds of organizations regarding critical infrastructure issues, including deep dives with partners in food and agriculture, healthcare/public health, emerging technologies, and the financial, energy, and transportation sectors; FVEYS and other foreign partners; and across branches of federal, state, and local government that had not previously implemented insider threat and/or OPSEC programs. This collaboration has resulted in the development of numerous resources — including the Safeguarding Science Toolkit and other sector specific implementation guides — that support public health and safety, and economic and national security, on a broad scale.

Because of the dedication of NCSC/ETD staff and the cooperation of our federal partners, we continue to achieve meaningful results.

Thanks to all of you for your partnership over the last few years. I can't wait to see what you do next!

Common Acronyms

CI - Counterintelligence

ETD - Enterprise Threat-Mitigation Directorate

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

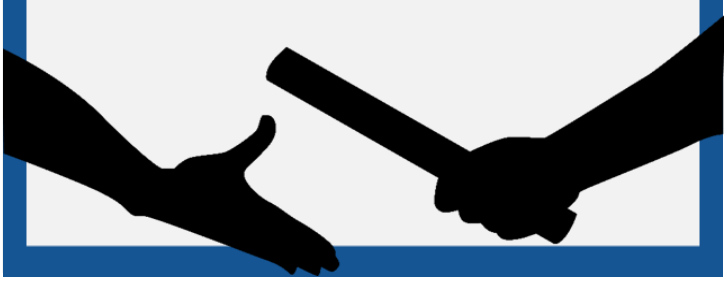
NT-50 - Non-Title 50

OPSEC - Operations Security

The NOP Has Fully Transitioned to NCSC!

The Interagency OPSEC Support Staff (IOSS) was part of the transition of mission resources for the National OPSEC Program move to NCSC. After the signing of NSPM-28 in January 2021, the IOSS team worked to provide training, documentation, resources, and support to NCSC to enable their successful standup of the NOP office within ODNI. It has been a long road, but we have reached our goal and IOSS support was an integral part of these efforts!. As of 31 December 2022, IOSS has officially been decommissioned and all OPSEC training and resources are now the full responsibility of the NCSC.

We would like to recognize all of the contributions to the OPSEC community that the IOSS provided during more than 34 years of service protecting our country. As we look to the future, we will not forget the efforts of so many OPSEC professionals who worked in the IOSS and helped to safeguard and protect our country from adversaries. With gratitude, thank you IOSS for all that you have done!



Nominations Deadline: Insider Threat Community Recognition Program

The 2023 Federal Counter Insider Threat Community Recognition Program is accepting nominations through 28 February 2023. Late submissions will not be accepted, so please submit early.

This annual non-monetary, 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 or agency Insider Threat Programs and associated personnel. The NITTF, OUSD(I&S), and DHS encourage individuals and teams to submit in the following categories:

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

Please contact Caren M. Roushkolb (carenmr@dni.gov) or Betsy York (betsyy@dni.gov) of NCSC/ETD if you have any questions or need the submission guide and forms.

PRACTICING DIGITAL DISCERNMENT

The Threat Lab | PERSEREC

Information that is incorrect or under-researched and articles that sensationalize, use emotional manipulation, and play on people's fears are prevalent in many of the online spheres people engage with daily. In collaboration with DoD's Counter-Insider Threat Program and the NITTF, the Threat Lab has created a graphic novel, ***Digital Discernment***, to raise awareness of the tactics and features that make Internet disinformation and misinformation so compelling, and to present strategies for evaluating content consumed online.

To protect yourself against misinformation, it pays to be an active participant in the media you consume. We all have busy lives, and it can be exhausting to investigate everything you read with a fine-tooth comb to see what is true or not. Instead, you can follow a simple checklist of questions to ask when you're consuming any media:

Purpose: What is the aim of the author making a claim? Are they trying to influence my emotions or provide accurate information?

Author: Who made the claim, and does the person have qualifications to make that claim? If they do have qualifications, are they the right qualifications to make the claim?

Relevance: Do the claims being made apply to you? Are the claims matching with the sources cited?

Currency: Is the claim being made up-to-date with information, or are there more recent updates? Has newer information come out that contradicts earlier information?

Sources: Are there good references and do well-qualified individuals agree with the claims?

Unless you're a total star, you won't have time to ask every single question, but it is important to try! By simply asking a few questions, you might find that you're better able to detect when a claim is trying to influence you. Awareness of emotional manipulation is key to not falling for misinformation!

the ThreatLab
Integrating Research Into Practice

To learn more, download the graphic novel at https://www.dhra.mil/PERSEREC/Selected-Reports/#PA-22-16

CDSE Insider Threat Vigilance Campaign 2023

Cashmere He
Center for Development of Security Excellence (CDSE)
Insider Threat Program

Regular messaging through communication and awareness materials can reinforce annual insider threat awareness training and help ensure the workforce is prepared to recognize and respond to the insider threat.

This response may include options to report concerning behavior or offer support to a colleague in need of assistance.

For the 2023 Insider Threat Vigilance Campaign, CDSE will be promoting a different theme each month and publishing or distributing awareness materials relevant to that theme in unique ways throughout the year. Use this campaign or consider tailoring it to your organization with resources from our website (https://www.cdse.edu/Training/ Toolkits/Insider-Threat/).

2023 INSIDER THREAT VIGILANCE CAMPAIGN

MONTH	FOCUS	TOPIC	RESOURCE	LINK
JAN	Report	Security and Compliance Incidents	Game: Adventures of Earl Lee Indicator: Mission One	https://securityawareness.usalearning.gov/cdse/multimedia/games/escape/index.html
FEB	Support	Operational Security	What Security Officers Need to Know About Probability, Voices From the SBS Summit Podcast	https://anchor.fm/threatlab/episodes/What-Security-Officers-Need-to-Know-About-Probability-e112d5g
MAR	Report	Foreign Influence / Preference	Case Study: Meyya Meyyappan	https://www.cdse.edu/Portals/124/Documents/casestudies/meyya-meyyappan.pdf
APR	Support	Cultural Awareness	Cultural Competence and Insider Risk Job Aid	https://www.cdse.edu/Portals/124/Documents/jobaids/insider/Cultural-Competence-and-Insider-Risk.pdf
MAY	Report	Threats of Violence	Video: Witting and Unwitting: Overlooked	https://www.dvidshub.net/video/862223/cdse-witting-and-unwitting-overlooked
JUN	Support	Resilience	"Working Together," Building an Infrastructure for Workplace Resilience Infographic	https://www.cdse.edu/Portals/124/Documents/jobaids/insider/working-together-infographic.pdf
JUL	Report	Unexplained Affluence	Potential Risk in Informal Banking and Finance Job Aid	https://www.cdse.edu/Portals/124/Documents/jobaids/insider/Potential-Risk-in-Informal-Banking.pdf
AUG	Support	Critical Thinking	Deepfakes and Unintentional Insider Threats	https://vimeo.com/602102971/f1f1012cf5
SEP	Report	Targeting by Adversaries	Academic Solicitation Short	https://securityawareness.usalearning.gov/cdse/multimedia/shorts/academic-solicitation/story.html (Copy and paste URL into the address bar of your web browser.)
OCT	Support	Cyber Threat Awareness	An Insider's Digital Footprint and Associated Risk Job Aid	https://www.cdse.edu/Portals/124/Documents/jobaids/insider/insiders-digital-footprint.pdf
NOV	Report	Unauthorized Disclosure	Case Study: Henry Frese	https://www.cdse.edu/Portals/124/Documents/casestudies/case-study-henry-frese.pdf
DEC	Support	Reporting	Supporting through Reporting Poster	https://www.cdse.edu/Portals/124/Documents/posters/small/Supporting-through-Rep.pdf

CDSE Center for Development of Security Excellence LEARN. PERFORM. PROTECT.

Counter-Insider Threat Certification News

Congratulations to the candidates who passed the Fall 2022 Certified Counter-Insider Threat Professional (CCITP) exam! NITTF and OUSD (I&S) will soon welcome 74 additional professionals into a community that currently includes 548 professionals certified in CCITP-Fundamentals (CCITP-F) and another 228 certified in CCITP-Analysis (CCITP-A). Conferrals will be processed by the end of January.

The spring registration will be open 13 February 2023 thru 31 March 2023. Certified professionals can update and track their professional development units (PDUs) online. You can also update PDUs, check your certification expiration date, and submit your plan at https://cint-gsx.learningbuilder.com.

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

UPCOMING OPERATIONS SECURITY TRAINING & INSIDER THREAT HUB OPERATIONS TRAINING

These events are open to stakeholders in the US Government. All classes are Eastern Standard Time and taught using Microsoft Teams — an account is not necessary. Please visit our website for more details. Registration requests received prior to the registration opening date will not be considered.

Note: In the subject of the email, please use REGISTARTION FOR [COURSE TITLE AND DATE]. For the Hub Operations Course, the email must come from a supervisor; for OPSEC Courses, the attendee may send the email.

Email ETD_REGISTRAR@dni.gov and include the following information:

1. Course title and date
2. Name
3. Work email
4. Department or agency

OPSEC Analysis (OPSE-2380)

Attendees will be able to develop critical information lists and determine the value of each item, identify threats and their values, identify common vulnerabilities and their values, calculate estimated risk, and determine viable countermeasures for reducing risk.

14-15 Feb. (0800-1600) - Registration opens 3 Jan.
21-22 March (0800-1600) - Registration opens 7 Feb.
6-7 June (0800-1600) - Registration opens 25 April

OPSEC Program Management (OPSE-2390)

This course provides learners with the knowledge needed to develop and sustain an effective OPSEC program. Prerequisite: OPSE-2380, OPSEC Analysis

16 Feb. (0800-1600) - Registration opens 3 Jan.
23 March (0800-1600) - Registration opens 7 Feb.
8 June (0800-1600 - Registration opens 25 April

OPSEC and Public Release Decisions (OPSE-1500)

This course addresses OPSEC issues that should be considered when reviewing information for public release and public access.

17 May (0800-1600) - Registration opens 5 April
27 June (0800-1600) - Registration opens 16 May

OPSEC and the Internet (OPSE-3500)

This course introduces learners to common threats, vulnerabilities, and countermeasures associated with the Internet.

15-16 March (1000-1400) - Registration opens 1 Feb.
10-11 May (1000-1400) - Registration opens 29 March

Insider Threat Hub Operations

This course introduces and exercises the basic functions of an insider threat program's centrally managed analysis and response capability to gather, integrate, analyze, and respond to potential insider threat information derived from counterintelligence, security, information assurance, human resources, law enforcement, and other internal and external sources. Please see our website for the full list of prerequisites.

7-8 March (0800-1600) - Registration opens 31 Jan.

Certified Counter-Insider Threat Professionals

These events may count towards professional development units! Log into your account or learn more about certification maintenance.

WELCOME TO NT-50 OPSEC PROGRAMS

If you are getting started or looking to improve your program, please register for OPSE-2380 *OPSEC Analysis* and OPSE-2390 *OPSEC Program Management*. These courses provide foundational knowledge and resources to establish and maintain an OPSEC program. These two classes also meet OPSEC personnel minimum training standard #2, "Developing and Maintaining an OPSEC Program."

Case Study: Jonathan and Diana Toebbe

S. Rothberg | NITTF

The recent case of Jonathan and Diana Toebbe illustrates our government's continuing struggle with espionage and the dangers posed by trusted insiders. After the Toebbes plead guilty in August 2022, the pair was each sentenced to roughly 20 years in prison and fined approximately $50,000. Their case exemplifies ongoing challenges with identifying potential insider threats, and highlights the risk factors that may lead an employee to commit espionage. It is also a stark reminder of the importance of protecting critical information through the implementation of OPSEC.

> Jonathan and Diana Toebbe were sentenced to roughly 20 years in prison and each was fined some $50,000.

In December 2020, FBI agents posing as representatives of an unnamed foreign nation obtained a package containing U.S. Navy documents marked as CONFIDENTIAL, a letter with instructions, and a Secure Digital (SD) memory card. This led to an undercover operation where the FBI maintained contact via encrypted emails with a subject known as "Alice," who provided confidential documents on US Naval submarines in return for payment. On 26 June 2021, the FBI set up a dead-drop with Alice where they observed Jonathan Toebbe, a nuclear engineer for the Navy with a Top-Secret security clearance, utilize the dead-drop while his wife, Diana Toebbe, acted as a lookout. At the dead-drop, the FBI found an SD card, later confirmed to contain restricted data about submarines. The FBI continued to set up future exchanges where Jonathan Toebbe would pass along confidential documents and information pertaining to US Navy submarines. In October 2021, Jonathan and Diana Toebbe were arrested and charged with conspiracy to share restricted data in violation of the Atomic Energy Act. After a long trial and numerous rejected plea deals (Politico), the couple ultimately pleaded guilty.

It has since been reported that Jonathan Toebbe actively approached senior officials from another country in April 2020, believing the foreign representatives would be eager to purchase the documents he had stolen.

Jonathan and Diana Toebbe, 2022

One senior official claimed that they had received a letter from Toebbe offering to sell them thousands of pages of classified documents pertaining to nuclear reactors. The senior official then gave the letter to the FBI, who then prepared to intercept the package sent by the Toebbes in December (New York Times). The senior official stated that they decided to cooperate with the FBI due primarily to the friendly relations between the FBI and their intelligence services (The Guardian).

The Toebbe case is a key example of the continuing struggle with potential insider threats. It is possible that insider threat-related indicating factors preceding the couple's choice to commit espionage could have been recognized and addressed before they become insider threats. For example, the Toebbes spoke out about feeling "anxious" about the nation's political climate, citing this as one of the reasons they decided to begin selling secrets. Additionally, Jonathan had been struggling with mental health issues and alcoholism prior to his espionage, while monetary issues played a role and the couple ultimately sold the secrets in exchange for $100,000 in cryptocurrency (Politico).

But were these indicators obvious enough to raise alarms, or were they so subtle, hidden (i.e., the crypto transaction), or even protected (i.e., the Toebbes' free speech rights) that it would have been difficult to view the indicators as real threats? Ultimately, balancing the necessary legal obligations, civil liberties, and other factors make the job of an insider threat professional challenging.

This case exemplifies the importance of continuously implementing OPSEC guidelines and strategies to protect the Nation's assets from the ongoing problem of insider threats. Developing a mindset and culture for safeguarding critical information within the workplace is a vital step in protecting agencies from insider threats. This case could have played out very differently had the Toebbes approached a different foreign entity – one that would have eagerly acquired the secrets without notifying US intelligence. Everyone plays a role in effective OPSEC and insider threat detection, and it is up to each agency to protect their critical information from both external and internal threats.

Case Study: The Acquisition of Twitter

S. Rothberg | NITTF

The recent acquisition of Twitter provides insider threat and OPSEC professionals with what might be the most wide-ranging exemplar of insider threat and OPSEC-related equities. Developments related to the Twitter acquisition have allowed us to see, through publicly available information, the impacts of historical company business decisions, leaks, mis/disinformation, insider threats, and OPSEC practices that affect current business decisions and actions, in real time. These "lessons learned" can help insider threat and OPSEC professionals increase their skills and subject matter knowledge, resulting in greater effectiveness of insider threat and OPSEC programs across the US Government and private sector.

OPSEC and the Protection of User Information

Long before Elon Musk agreed to purchase Twitter, the social media platform was facing scrutiny over its cybersecurity practices and its ability to protect user data. These concerns have grown since Musk's takeover, especially after he reportedly instituted major layoffs. The history of Twitter cybersecurity issues paired with sweeping changes impacting employees should have Twitter users asking basic OPSEC questions about how their information is being protected, and more importantly, what steps users can take to protect their data.

Twitter has a long history of cybersecurity issues when it comes to protecting user information. The FTC and

the Department of Justice accused Twitter of mishandling users' personal information from May 2013 through September 2019, leading to Twitter's agreement to pay a $150 million settlement. In July of 2022, Twitter suffered from a cybersecurity breach that resulted in 5.4 million Twitter profiles having their email addresses and phone numbers exposed. To further cement Twitter's ongoing problems with cybersecurity, the former security chief at Twitter, Peiter Zatko, testified before the Senate Judiciary Committee in September 2022 about the security issues at Twitter. Zatko claimed his January 2022 firing for "poor performance" was retaliation for raising security weaknesses with Twitter's board. Zatko pointed out that an alarming number of Twitter employees had access to user data and that the company's "lax" security made Twitter vulnerable to infiltration by a foreign entity (USA Today).

Given Twitter's history regarding data and cybersecurity issues, many users have raised concerns about the potential changes Musk will make to either hinder or strengthen Twitter's security practices. These are prudent questions to ask when new changes are rolled out on any platform that collects personal data. Another potential concern relates to proposed plans to add features and fees to the platform, which would require users to share financial information and bank account numbers with Twitter. Other changes, such as laying off Twitter's employees, raise concerns about the skillsets and number of personnel on the security team. Additionally, Musk's foreign connections to countries such as China, where Tesla conducts sales and production activities, could be an issue, especially if the concerns regarding potential foreign access to Twitter information turn out to be accurate.

It remains to be seen what Twitter will do to protect user data. It is just as likely that Musk's acquisition of the social media platform will lead to greater cybersecurity protections for users, especially given that Musk has resources he can bring to bear to address Twitter's historical (and current) security problems. In the meantime, it's important for users to understand how they can protect their own data, regardless of who is in charge of the platform. Actions such as deleting old tweets, checking privacy settings, and paying attention to the information users are tweeting are prudent ways for users to protect personal information. When on Twitter, or any social media and online platform, users should be cautious about what they are posting and what type of information they are sharing.

Twitter's Potential Insider Threats

Do Twitter employees pose an insider threat to the social media giant? As frequent readers of this newsletter, you are aware that an insider threat is anyone with access to an organization or company who may use that access, either wittingly or unwittingly, to harm the organization. Harm can include malicious, complacent, or unintentional acts that negatively affect the integrity, confidentiality, and availability of the organization, its data, personnel, or facilities. This would certainly include both current and former Twitter employees, one of which was recently sentenced to 3.5 years in prison for acting as an agent for Saudi Arabia, sharing personal information of users of interest to Saudi officials.

The compromise of proprietary information can be devastating to any company, and Twitter is no exception. As previously noted, Mr. Zatko (a whistleblower[1]) filed a complaint with the FTC, SEC, and DOJ, alleging that Twitter employees were installing non-approved computer software, deactivating software updates, turning off firewalls, enabling remote desktop use for non-approved purposes, and intentionally installing spyware on their work computers at the request of outsiders. Such actions not only violated Twitter policy, they were also indicative of a potential insider threat. Equally concerning is reporting by CNET alleging India was able to place two agents on Twitter's staff, and claiming the FBI notified Twitter that at least one Chinese agent had infiltrated the company.

Perhaps in an effort to get ahead of these problems, Twitter owner Musk has reportedly promised legal action against employees who willfully violate the terms of their signed nondisclosure agreements. The New York Post reports that Musk advised his workforce, "This will be said only

once: If you clearly and deliberately violate the NDA you signed when you joined, you accept liability to the full extent of the law & Twitter will immediately seek damages." Whether this is an effective method for addressing insider threat challenges remains to be seen, but what is evident is the fact that Musk takes the hazard posed by malicious insiders very seriously. In light of the security lapses noted above, failure to properly "exit" staff who are being fired or released can create a host of potential insider threats among those who are disgruntled due to their own firing or the firing of their coworkers.

The Proliferation of Mis/Disinformation related to Twitter

News regarding Twitter currently seems to fall within the "Wild, Wild West" of mis/disinformation – anything and everything regarding Twitter and Elon Musk is open for debate, no matter how outlandish. On some days, the news changes by the hour, and changes so fast that it is difficult for the average reader to keep up. In many cases, the source of the information is not readily apparent, the motivations of the source have not been determined, and the veracity of the information has not been proven. For example, in response to a recent media report suggesting Twitter was down to 1300 employees, with 130 of those authorized to move over from his other companies, Musk tweeted that Twitter has "~2300 active, working employees," adding "less than 10" of those were from Tesla, SpaceX, and The Boring Company.

As we noted in our July 2022 Newsletter article entitled "Critical Thinking and Mis/Disinformation," false or misleading information can take almost any form and come from any source. In addition, it's easy for anyone to join the conversation/debate on the Internet, no matter their level of expertise on any given topic. Unfortunately, emotions regarding the Twitter purchase seem to be running high, with one of the major fractures split along political lines. This has the possibility to enflame emotions among Twitter employees, Twitter users, and everyone in the general public who is following Twitter news. And as noted in the Toebbe case summary in this issue, political considerations – which are shaped by what we see and hear from our news sources - could be a motivating factor in becoming an insider threat.

As OPSEC and insider threat professionals, we are obligated to provide the very best security advice and guidance to the leaders of our organizations. Staying abreast of current and emerging security challenges in an ever-changing threat landscape is not easy, and while knowing how to mitigate such dynamic threats is even trickier, watching how others handle problems threatening their respective organizations can be instructive and worthwhile. Ultimately, perhaps we can learn from ongoing current events in order to get ahead of our own organization's insider threat and OPSEC challenges, before they cause irreparable harm.

[1] *Whistleblowers exercising their legal rights are NOT insider threats*

Understanding the Impact of Organizational Justice on Insider Threat

Dr. Chloë Wilson | ODNI

The following excerpts are from the article "Exposing the Cracks: Impact of the COVID-19 Pandemic on Organizational Justice in the Intelligence Community" written by Dr. Chloë Wilson, a research psychologist with ODNI. The article was published in the December 22 issue of Studies of Intelligence.

Just as the terrorist attacks of 9/11 forced the Intelligence Community to recognize the critical need for integration, the COVID-19 pandemic is another catastrophic event that should prompt self-reflection within the IC. While the pandemic has produced new diverse challenges for organizations to counter, it has simultaneously exacerbated already existing and overlooked issues within the IC. One of the existing issues is the division between supervisors who embrace, and those who neglect, fostering a culture of organizational justice.

Organizational justice was first defined by organizational researcher Jerald Greenberg as "people's perceptions of fairness in organizations along with their associated behavioral, cognitive, and emotional reactions". Organizational justice refers to an individual's tolerance for observed fairness. Whether or not the outcome or decision is fair is less important than whether employees *perceive* it as fair. Although organizational justice is not a new term in organizational psychology or intelligence literature, the COVID-19 pandemic has brought about new circumstances that have heightened perceptions of injustice for employees.

Organizational justice refers to an individual's tolerance for observed fairness. Whether or not the outcome or decision is fair is less important than whether employees *perceive* it as fair.

Organizational justice is a cause for concern for the IC, as employee disgruntlement has been highlighted as a leading factor of insider threats. Research by the CERT Program at Carnegie Mellon assessed the series of events that occurred before engaging in insider threat, 17 percent

of the cases showed evidence of disgruntlement leading up to their transfer of classified information. Further, other researchers have highlighted that workplace disgruntlement and employee dissatisfaction were identified as the two key underlying causes of deviance in the workplace and organizational crime.

Insiders engage in deviant behavior as a way of restoring the balance of fairness, taking revenge for perceived injustices they experienced. For example, many case studies highlight that workplace deviance is often preceded by negative experiences, such as a poor performance review, dispute with coworkers, or unfavorable relocation. Researchers at the US Secret Service and Carnegie Mellon found that of the 49 cases of insider sabotage in their sample, 88 percent of the perpetrators held a "work-related grievance" before the act of sabotage.

> Organizational justice is a cause for concern for the IC, as employee disgruntlement has been highlighted as a leading factor of insider threats.

Therefore, in reflecting on the variety of workplace changes that have been brought about by the COVID-19 pandemic, the conditions for perceptions of unfairness have only increased. Beyond the obvious devastation, anxiety, and ambiguity surrounding the virus transmission, employees worked through resource and personnel shortages, virtual environments, and strained communication channels. Workers experienced new circumstances that called into question the fairness of procedures and treatment of employees furthering the divide between supervisors who exhibit the principles of organizational justice over those who do not. The article highlights four vignettes demonstrating the various circumstances that employees experienced organizational injustice while working during the initial months of the pandemic and discusses the implications of those decisions.

Although organizational injustice often serves as an aggravating factor to insider threat, supervisors who demonstrate organizational justice in their actions can also serve as a protective factor in times of stress. Within the *Critical Path to Insider Threat*, Shaw and Fischer[1] noted that most of the insider threats in their study could have been prevented by timely and effective action to address the anger, pain, anxiety, or psychological impairment of perpetrators who exhibited signs of vulnerability and risk well in advance of their crime. Additionally, the authors describe how insiders often experience a major change in their life (e.g., death of a loved one, divorce, organizational relocation or restructuring) that in combination with poor management facilitated an insider further down the path.

Both the government and private sector have fallen victim to problematic behavior like employee retaliation. While selection and screening precautions can help filter out bad actors, individuals who were once trustworthy employees can experience a triggering event at work that impacts their loyalty. Thus, ensuring that supervisors understand and implement organizational justice principles are paramount in deterring insider threats. Through their actions, supervisors have the ability to influence how employees feel valued and supported at work. How supervisors communicate information, enforce policies, endorse assistance, and treat personnel can cause employees to contemplate the equity in decision making and the conduct of the organization.

Although it is not yet known what the impact of the pandemic is on insider threat in the IC, industry has reported a significant increase in insider cases over the past two years[2] [3] [4] (e.g., Cybersecurity Insiders, 2021; Gips and Trzeciak, 2022; Ponemon Institute, 2022). One study reported that employees are 85 percent more likely to leak files today than they were pre–COVID-19 (Code42, 2021). The findings from industry, in combination with the anecdotes from the article, are concerning. If employees are more likely to leak than prior times, supervisors are more important than ever in ensuring organizational justice for their employees.

Endnotes:

1. Shaw, E. & Sellers, L. (2015). Application of the critical-path method to evaluate insider risks. Studies in Intelligence, 59(2), 1–8.
2. Cybersecurity Insiders. (2021). 2021 Insider Threat Report. https:// www.cybersecurity-insiders.com/ portfolio/2021-insider-threat-report-gurucul/
3. Gips, M. & Trzeciak, R. (2022). The insider threat: What hath COVID -19 wrought? Global Security Exchange. https://www.gsx.org/ gsx-blog/the-insider-threat-what-hath-covid-19-wrought/
4. Code42. (2021). 2021 Data Exposure Report (1–15). Ponemon Institute. https://www.code42.com/resources/reports/2021-data-exposure

Navigating Enterprise Threat Mitigation in the 21st Century

Robert W. Rohrer
Assistant Deputy Secretary
for National Security
Department of Health and Human Services

When federal policymakers chose the National Counterintelligence and Security Center (NCSC) to lead a newly revised National OPSEC Program, the intent was not to create a new task force, or more silos in a community of silos, but to offer at-risk communities and sectors a hand in integrating OPSEC principles with other defensive efforts.

A year ago, NCSC released a new "Enterprise Threat Mitigation" (ETM) framework depicting the OPSEC cycle as a risk management cycle that considers adversarial threat in the calculation of risk. The ETM framework aligns OPSEC with Enterprise Risk Management (ERM) practices proscribed in Office of Management and Budget (OMB) Circular 123, ideally leveraging federal ERM councils to promote executive-level decision-making that best counters the risk posed by adversarial threats. In practice, such decision-making is optimized when senior OPSEC officials are positioned within the organization to have access to the most senior leadership, as required by NSPM-28. Even then, senior officials are challenged to work effectively with leadership across the organization in a way that compliments stated goals and objectives.

> Such decision-making is optimized when senior OPSEC officials are positioned within the organization to have access to the most senior leadership.

Three suggestions as we forward with these efforts –

First, **words matter**. There is a danger of convoluting risk, threat, and vulnerability, but the terms are not interchangeable. Risk is a function of threat, vulnerability, and consequence. When those in the national security field speak of "foreign adversarial threats," we are speaking of Advanced Persistent Threats (APTs) from a state or non-state actor. In other words, these are well-resourced and coordinated external threats, with strategic goals contrary to our national interest. When we speak of mitigation, we are largely referring to efforts to minimize vulnerabilities. Vulnerability is often an internal organizational challenge, and subject to its "control" (a term often used to describe mitigation practices).

> Example: The insider threat community still struggles with terminology. Practitioners often debate whether the problem should be referred to as "insider threat" or "insider risk." In reality, a trusted insider is not the risk, but could be a threat or a vulnerability depending on intent. The lone-wolf insider, as seen in the most egregious unauthorized disclosure cases, is a "threat" because of an intent to exploit trust and cause organizational harm. The unwitting victim of a spear-phishing attack is not a "threat" but a vulnerability exploited by an external threat. It could be argued that even a recruited agent of an adversary is more of an exploited vulnerability (behind all notorious American spies were foreign case officers). The "risk" is that the trusted insider (as a threat or a vulnerability) will take some form of action that has significant "consequences" – arguably the most important risk calculous factor.

When speaking to enterprise risk management professionals in executive leadership, such as chief operating officers, program directors, and staff directors, it is important to speak to the threat in a way that helps calculate the enterprise risk. It's also important to note that the APT of our greatest power competitors is not one siloed risk. It is something that will play into risk calculus across many, if not all, programmatic and organizational priorities.

Second, **understand your role**. We are seldom the risk owners. As national security professionals, our job is to understand the THREAT- intent (strategic goals) and capability (tactics, techniques, and practices) - even if we do not own the organizational risk. Depending upon our larger organizational role, we may play a pivotal role in mitigating the threat though personnel security and insider threat programs, supply chain risk management, physical and technical countermeasures, and so on. But we typically do not own the overall risk for organizational programs and missions.

Finally, **understand competing interests among risk owners and work with them**. Resources for defending the enterprise are always limited, preventing us from defending everything against everyone. That said, we need to understand that enterprise risk management practices seek to help, not hinder, the protection of the most important organizational assets and resources. As national security professionals, it is our role to understand the capabilities and intent of our adversaries. To effectively advise risk management professionals, we do our best to understand what assets and resources are of most value to our adversaries and work with the risk owners to prioritize those for protection.

> Enterprise risk management practices seek to help, not hinder, the protection of the most important organizational assets and resources.

In summary, OPSEC principles are already incorporated into organizational ERM practices. Calculating risk requires an understanding of threat, organizational vulnerabilities, and the consequences of losing critical assets or resources. The challenge for national security professionals is ensuring that decision-makers understand the threat faced by our greatest power competitors, as well as the consequences we face as a nation when our resources and assets are compromised. To meet this challenge, we must effectively communicate with all stakeholders, articulate the threat in clear, unclassified terms that resonate with larger organizational goals, and continue to educate and improve our own understanding of organizational business practices.

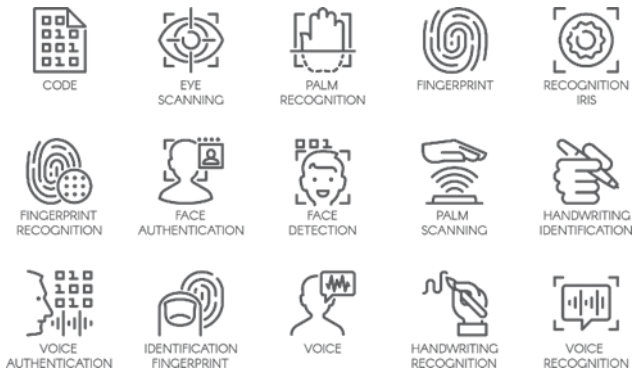
OPSEC 21ST CENTURY TOOLS & TECHNOLOGIES
- BIOMETRICS -
National Insider Threat Task Force

The biometric data we know today started being used in the first part of the 20th century with the advent of fingerprint technology. In 1903, New York State Prisons began using fingerprint technology for the identification of prisoners. By 1924, the Bureau of Investigations (now known as the FBI) began collecting and using fingerprints to assist local law enforcement with their investigations. In the 1960s, facial recognition technology started being used to automate facial identifications. Early use of biometrics was primarily used by the government.

Currently, biometrics refer to the process of measuring, recording, and analyzing physiological features. Certain physiological features are permanent and unique. These features are known as "biometric characteristics," and are measured by a sensor array and stored in a database as a template. This template is what allows biometric technology to verify your identity. Biometrics provide an accurate identification method to gain access to a device, facilities, and countries, and even trace lineage or track criminals. The main concern is the lack of regulations and laws about the use and storage of biometric data.

Today, biometrics are being used for a multitude of applications, not just by governments, but for commercial and individual purposes. Biometrics are being routinely used for identity and access management. Many companies are implementing biometric technology to allow employees to gain access to facilities. The federal

government collects and uses individual biometric data for processing migrants at border patrol facilities and many US residents opt into providing facial recognition, iris scans, and fingerprint technology to expedite their identity when arriving at US border entry and to expedite security lines at US airports. Smart technology users also use personal biometric features on their personal smart-devices. Many people are opting into implementing facial recognition or fingerprint technology to unlock their device for convenience, and an added layer of security.

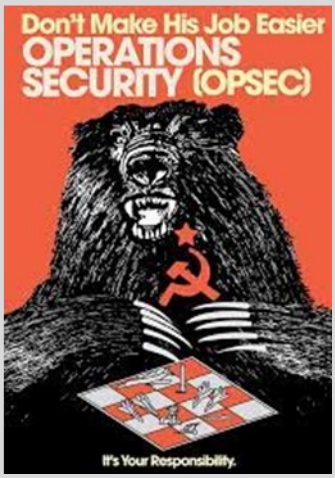


DNA sequencing is the most complete and accurate biometric marker to identify an individual. Law enforcement agencies will gather the DNA of criminals and store them in databases that can be accessed by those with authorization to do so. However, millions of people voluntarily deposit their DNA into commercial databases to trace ancestral heritage, identify their heritage, and create precise family trees.

There have been some regulations at the state level, with the Illinois state government implementing the Biometric Information Privacy Act in 2008, guarding against the unlawful collection and storing of biometric data. Several other states have followed suit, but there are no federal laws to govern the use and collection of biometric information. Personal identifiers could potentially be leaked, stolen, or sold to nefarious actors who could then replicate the biomarkers of an individual to gain illicit access, as there is a lack of regulations around biometric technology. However, law enforcement agencies routinely share access to their databases that contain biometric information that is typically only shared among other government agencies. Conversely, commercial and social media companies store users' biometric information without much regulation or legal constraints to govern as to how they may share biometric data.

It is important we ask what happens to the biometric data of individuals if a company is acquired by another company or by a foreign-owned entity. These are issues that people need to keep in mind when they think about sharing any personally identifiable/biometric data with commercial biometric vendors and federal government programs.

OPSEC Through the Years



Senior Official Performing the Duties of the Director of NCSC

In the span of roughly a week in November 2022, federal judges across the country sentenced defendants to prison in three high-profile cases that underscore the challenges posed by insider threats and the need for enhanced operations security (OPSEC) by government and industry organizations. One of those cases (the Toebbe case) is highlighted on page 7 of this issue. The others are as follows:

- On 16 November, a federal judge in Cincinnati sentenced Chinese intelligence officer Yanjun Xu to 20 years in prison after Xu targeted US aviation companies, recruited their employees to travel to China, and solicited their proprietary data on behalf of the People's Republic of China. Xu was the first Chinese intelligence officer to be extradited to the United States to stand trial.
- On 7 November, a federal judge in San Diego sentenced former US Army helicopter pilot Shapour Moinian to 20 months in prison after Moinian provided aviation-related materials from his US defense contractor employers to representatives of the Chinese government in exchange for money and lied on national security background forms.

We applaud the fact that these perpetrators were caught and punished for their crimes, but detecting and preventing sensitive data from being unlawfully disseminated in the first place must be a top priority for any organization that has information worth protecting.

This is a good time for all of us to revisit and improve our respective security postures. January 2023 is National OPSEC Awareness Month, a month-long communications campaign to help raise threat awareness and share risk mitigation practices across the executive branch and among trusted partners.

Throughout January, we encourage federal agencies and other organizations to get involved in National OPSEC Awareness Month to introduce OPSEC concepts to their respective workforces and to solicit the assistance of their workforces in protecting critical information. For information on OPSEC training, resources and templates, please visit NCSC's OPSEC webpage at: https://www.dni.gov/index.php/ncsc-what-we-do/operations-security.

Thank you.

Michael J. Orlando