May 2021 Volume 3 | Issue 2

FEDERAL PARTNERS NEWSLETTER

SPECIAL EDITION

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

What Makes A Defensive Counterintelligence Program Successful?

Brittany W., NCSC/FPG

Information of value to national security is no longer limited to the classified realm or contained within the traditional Intelligence Community (IC). Government departments and agencies that are not within the Department of Defense (DOD) or IC, known as Federal Partners, have assets and programs of interest to foreign adversaries. This leaves Federal Partners open to exploitation by foreign intelligence entities (FIEs) and provides a point of access to proprietary, sensitive, and classified information. Therefore, Federal Partners should identify the risks to assets critical to their mission which, if compromised, may damage national security. Building a defensive counterintelligence (CI) capability can help to mitigate risks.

There are common principles that define all successful defensive CI programs, regardless of how the individual organization tailors its specific program. These are:

- The Federal Partner's legal counsel should provide clear guidance on its CI program's activities.

UPCOMING EVENTS

- May 26 – Quarterly Federal Partners CI Roundtable
- June 14 – NITTF Unauthorized Public Disclosure Colloquium
- June 16 – NITTF Talk – Work-place Violence
- June 22-23 – NITTF Hub Ops Course (Registration Closed)
- June 28 – July 2 – Special Se-curity Officers Course (SSOC)*
- July 14 – NITTF Talk – Insider Threat Current Events
- August 30 – September 3 – Personnel Security Adjudica-tions Course (PSAC)*
- September 13-17– PSAC*
- September 20-24 – Sensitive Compartmented Information Facility (SCIF) Course*

* See Training Opportunities section for more information on page 6.

- Senior management should accept the purpose and principles upon which the Federal Partner's CI program is developed and provide appropriate support and resources to the program.
- The Federal Partner's senior CI official should have direct access to the department secretary or agency head so issues of national security may be addressed in a timely and discreet manner and with appropriate authority.
- The Federal Partner's CI program should have a centralized management structure rather than having different CI functions split among various departmental elements.
- The CI program must provide support to the entire department or agency, regardless of location, not just the headquarters.
- The CI program needs solid relationships within the department, especially with security, information assurance, inspector general, and human resource entities, and with appropriate elements in the intelligence and CI communities.

A defensive CI program may begin with a small, preliminary footprint with limited capabilities. In the early stages, this provides organizations with an initial capability to start building a culture of CI awareness in the department. As a defensive CI program matures, it is important that its scope and scale fit within the organization that it supports, and it be appropriately resourced to defend the organization and its employees against those FIEs that seek to harm U.S. national security interests.

Reference: CFIT Implementation and Best Practices Guide, 2016

"Federal Partners have assets and programs of interest to foreign adversaries."

USDA and the Protection of Intellectual Property and Proprietary Information

Keith McElfresh, Office of Homeland Security, USDA

Collaborations with foreign governments, institutions, and scientists are a critical component of the U.S. Department of Agriculture's (USDA) mission. However, they are not without risk. Foreign nations have a strong desire for classified and unclassified information related to U.S. economic, military, and foreign policy.

USDA is comprised of 29 agencies and offices, with nearly 100,000 employees who serve the American people, which includes more than 4,500 locations and more than 90 research locations across the world. USDA provides leadership on food, agriculture, natural resources, rural development, nutrition, and related issues through research and development, public policy, and the cultivation of foreign trade relationships. Ensuring the appropriate balance between collaboration and mitigating the potential vulnerabilities introduced is essential to the success of USDA's mission.

National Security Policy Memorandum 33 (NSPM-33), the United States Government-Supported Research and Development National Security Policy, provides a framework for USDA to identify and protect its most sensitive animal and plant research. USDA's Office of Homeland Security (OHS) and the Office of the Chief Scientist are working diligently with mission areas and agencies to identify and protect sensitive areas of research.

USDA's Agriculture Research Service (ARS) was the first USDA Agency to develop an internal review to identify research projects vulnerable to economic espionage. ARS considers this intellectual property that requires protection. The ARS-developed process will be expanded to apply to other USDA agencies as we continue to identify additional sensitive areas of research. Additionally, USDA's OHS is working with ARS to develop an online training module to

educate USDA staff on the ongoing threats to and protection of agriculture research information. These efforts also align with the strategic objectives of the U.S. National CI Strategy.

Transportation Security Administration's Counterintelligence Program

Nicholas Kimsey, CI Officer, DHS, TSA

The Transportation Security Administration (TSA) has established a counterintelligence (CI) program to protect TSA personnel, information, and critical assets from foreign intelligence threats. TSA's CI program focuses on awareness training tailored to each at-risk population, support and reporting that ranges from referrals of indicators to foreign travel deployment and foreign visitor engagement, analysis and production (including analysis supporting the Committee on Foreign Investment in the U.S. and Supply Chain Risk Management), and support to investigations through inquiries and referrals.

The successful creation of TSA's CI program came as a direct result of a year-long CI pilot program, conceived in 2019, that began with establishing roles and responsibilities across offices within TSA and concluded with the successful draft of CI policy documents needed for TSA to begin CI operations and functional services. In 2020, TSA received delegated authority from the Department of Homeland Security Secretary that allows TSA to operate independently on defensive CI activities. Following the Secretary's delegation, TSA issued CI credentials and a Field Reporter Number to its first CI Officer, which enabled full-spectrum CI coverage for the agency. One of the first efforts TSA's CI program accomplished, in conjunction with other TSA offices, was the creation of a critical assets list which includes facilities, equipment, networks, information, and populations that require persistent protection from insider threats and foreign intelligence entities. Looking ahead, TSA is projected to hire additional CI personnel by the end of calendar year 2021.

NCSC RESOURCES

» CFIT Implementation and Best Practices Guide

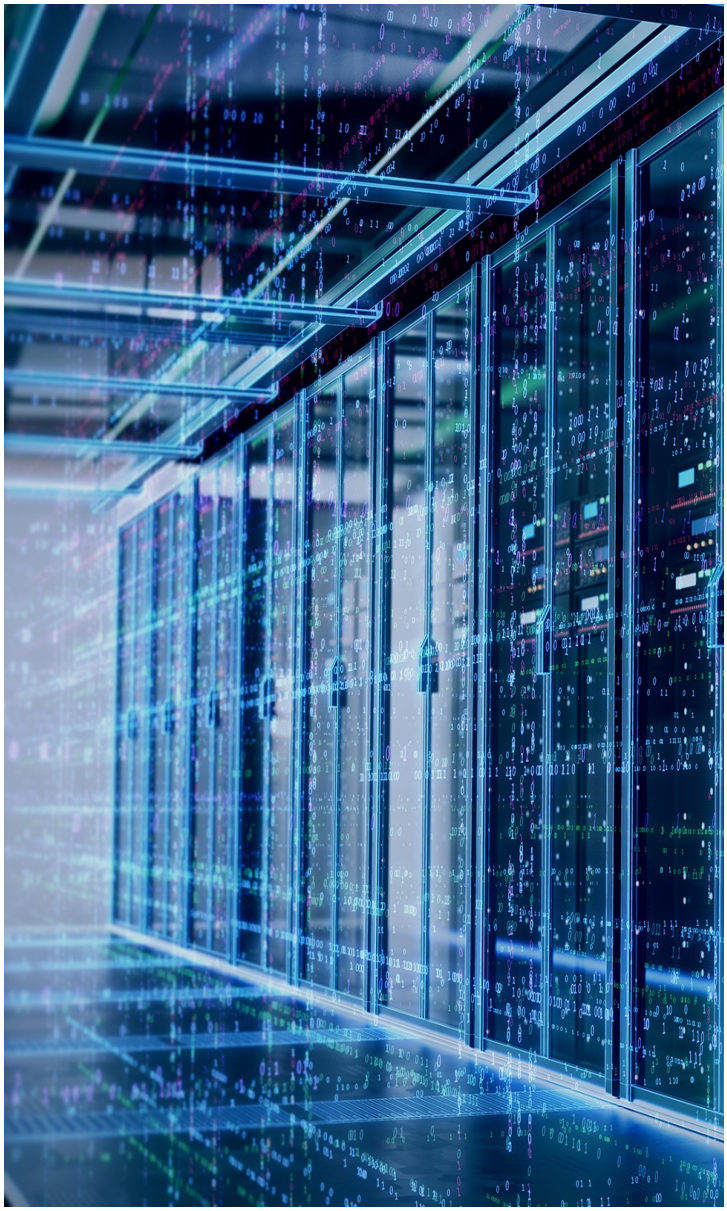
» DOE Cyber Vulnerability Testing and Enumeration Program, CyTRICS

» IT Sector Coordinating Council Supply Chain Resources (ONSAT)

» Supply Chain Risk Management

» Best Practices for Preventing Business Disruption from Ransomware Attacks

» Potential Threat Vectors to 5G Infrastructure



> “CI awareness is perishable and the threat from foreign intelligence services (FIS) must consistently be broadcast to the staff by way of awareness training, CI briefings, and agency-wide notifications.”

Counterintelligence During a Pandemic: Opportunities and Challenges

Lance English, CI Program Manager, NRC

The COVID-19 pandemic has provided new challenges and opportunities for federal agencies faced with a workforce who, by and large, are working from home but are still conducting the same sensitive work that was once performed in the office. Of the many challenges facing defensive counterintelligence (DCI) programs, like the one employed by the Nuclear Regulatory Commission (NRC), the most important is remaining vigilant to risks the staff face in conducting operations remotely. Another challenge is the need to continuously engage staff to maintain awareness of the threat from foreign intelligence services (FIS).

While foreign travel has been curtailed, international meetings and conferences are being conducted virtually, and at an even greater frequency than prior to the global pandemic. Existing pre- and post-travel counterintelligence (CI) questionnaires and briefings the NRC’s DCI used for overseas travel are less applicable to a meeting conducted virtually than to actual foreign travel.

CI awareness is perishable and the threat from FIS must consistently be broadcast to the staff by way of awareness training, CI briefings, and agency-wide notifications. Since the pandemic outbreak in March 2020, the NRC DCI program has issued three agency-wide announcements to staff related to CI concerns while using virtual platforms, and FIS online targeting of government employees and clearance holders. The DCI program has also participated in NRC regional office all-hands meetings, briefing CI awareness to staff in these geographically separate locations.

As the program manager for the DCI program at NRC, I look frequently to the online SAGE platform for help in finding contacts in other federal agencies with expertise for collaboration, and relevant information to share with our staff regarding CI concerns or FIS methodology. I welcome the opportunity to engage with any of the members of this community directly in sharing lessons learned, additional resources for consideration, and working cooperatively to advance CI awareness across the interagency.

NCSC Insider Threat Directorate and National Insider Threat Task Force

Adam C., Insider Threat Directorate & National Insider Threat Task Force, NCSC

The National Counterintelligence and Security Center (NCSC) Insider Threat Directorate (ITD) and National Insider Threat Task Force (NITTF) orchestrate a number of educational and awareness initiatives such as Insider Threat Hub Operations Courses, virtual NITTF Talk series (i.e., timely discussions with experts regarding insider threat-related topics), and the NITTF Newsletter.

In the next few months, the following NITTF offerings will be available:

» **June 16**
NITTF Talk – Insider Threat Current Events

» **June 22-23**
NITTF HUB Ops Course
(Registration Closed – Class Full)

» **July**
NITTF 3rd Quarter Newsletter Published

» **July 14**
NITTF Talk – Insider Threat Current Events

To participate in these events, please reach out to NITTF-Assistance@dni.gov.

Also note that during September 2021, NCSC will work collaboratively with departments and agencies across the federal government to support the third annual National Insider Threat Awareness Month (NITAM), which emphasizes the importance of safeguarding our nation by detecting, deterring, and mitigating insider threats. All Executive Branch departments and agencies were sent an executive memo from the Acting Director/ NCSC emphasizing the importance of participating. Information and details regarding NITAM events will be available in July.

Preparing for National Operations Security (OPSEC) Program Requirements

Michelle A., EdD, National OPSEC Program Office, NCSC

National Security Presidential Memorandum 28 (NSPM-28), the National OPSEC Program contains new requirements for all departments and agencies. To prepare to adopt these changes, there are resources already available to support your organizational needs.

As the National Counterintelligence and Security Center (NCSC) prepares to integrate the Interagency OPSEC Support Staff (IOSS) functions from the National Security Agency (NSA), IOSS staff continue to conduct historical activities which include virtual and self-conducted courses for program managers, practitioners, and general awareness; training and awareness materials for distribution; and other information references. This information is available by registering on the **http://www.ioss.gov** website. NCSC is also integrating OPSEC into its outreach activities to create a synchronized approach to OPSEC development, collaboration, and feedback processes. In the meantime, if your organization would like to learn more regarding OPSEC changes and get started, contact us through NCSC_FEDS@dni.gov.

Training Opportunities

Personnel Security Adjudications Course (PSAC)

PURPOSE
This curriculum prepares security specialists to conduct adjudications of covered individuals to determine eligibility for initial or continued access to classified national security information or eligibility to hold a sensitive position in accordance with Intelligence Community Directive (ICD) 704 and Security Executive Agent Directive (SEAD) 4 guidelines. This program is also essential for security specialists from other security disciplines who need to better understand how their work directly supports national security eligibility determinations.

WHEN
30 August - 3 September 2021; or
13-17 September 2021;
4 hours per day (AM or PM)

WHERE
Virtual instructor led via Webex

REGISTER
Please contact NCSC-Training@dni.gov to register.
There is limited seating for this event.

Sensitive Compartmented Information Facility Course (SCIF)

PURPOSE
This course will give you a better understanding of Intelligence Community (IC) physical security policies and prepare you to implement the requirements of the IC 705 series documents (ICD 705; ICS 705-01; ICS 705-02 and the ICD 705 Technical Specifications). The program also stresses the Life Cycle of a SCIF; design, construction, best practices and operations for a SCIF from cradle to grave and includes a security panel forum compromised of representatives from several IC element Accreditation Offices.

WHEN
20-24 September 2021; 4 hours per day (AM or PM)

WHERE
Virtual instructor led via Webex

REGISTER
Please contact NCSC-Training@dni.gov to register.
There is limited seating for this event.

Special Security Officers Course (SSOC)

PURPOSE
Security professionals who are responsible for the day-to-day management and oversight of Sensitive Compartmented Information (SCI) indoctrinated personnel, SCI facilities, and/or SCI programs are encouraged to attend this training. During the course, attendees receive an overview of personnel, physical, and Information security disciplines, practical exercises, and real-life scenarios.

WHEN
28 June – 2 July 2021; 4 hours per day (AM or PM)

WHERE
Virtual instructor led via Webex

REGISTER
Please contact NCSC-Training@dni.gov to register.
There is limited seating for this event.

From the Acting Director

Michael J. Orlando
Acting NCSC Director

The United States is facing increasingly aggressive threats from foreign state and non-state actors who are launching more complex and creative attacks on American government and industry, from our supply chains to our health care systems. Almost all U.S. Government (USG) agencies, including non-national security agencies, are being targeted along with private sector companies, academic institutions, and national laboratories. These targeting activities range from cyber intrusions to supply chain attacks, insider threat activities, economic espionage, and traditional espionage, or a combination of them all.

Given this evolving threat landscape, strong relationships between federal partners are more important than ever. The 2020 breach of multiple networks across the USG and private industry by Russian intelligence hackers demonstrates just how critical it is to partner to protect our collective systems, infrastructure, and people. The National Counterintelligence and Security Center (NCSC) is committed to leading and supporting the USG in strengthening counterintelligence (CI) and security activities and programs to protect our nation.

> *"Almost all U.S. Government (USG) agencies, including non-national security agencies, are being targeted along with private sector companies, academic institutions, and national laboratories."*

To help strengthen our collective security, NCSC is declaring May as Federal Partners Month! Federal Partners Month will help bring attention to the threats posed to Non-Title 50 organizations and seek to highlight the importance of a well-developed and proficiently executed CI and security program. The NCSC Federal Partners Group (FPG), along with our NCSC colleagues, will assist our partners in making improvements to their CI programs by helping to identify gaps in information and provide resources and assistance in the implementation of effective solutions.

Follow us on **Twitter @NCSCgov** to see the NCSC FPG's Defensive CI Tip of the Week for Federal Partners Month. For more information on NCSC CI and security topics, please visit our website at **https://www.NCSC.gov**. For questions about support and information available to Federal Partners, please email FPG at **NCSC_FEDS@dni.gov**.

Michael J. Orlando