FEDERAL PARTNER NEWSLETTER

Volume 2 | Issue 3
December 2020

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

Non-IC JDA Process and Opportunities

Joint Duty Program Office, ODNI

In 2017, the Intelligence Community (IC) Chief Human Capital Officers Council (CHCO) allowed for the advertisement of Non-IC positions on the Joint Duty Application Tool (JDAT). The Intelligence Community Directive (ICD) 660 and Intelligence Community Policy Guidance (ICPG) 660.1 allow for the detail of IC civilian personnel to positions in other IC elements or relevant organizations that provide IC Joint Duty qualifying experiences. The process for a Non-IC organization to obtain resources through an IC civilian Joint Duty Assignment (JDA) includes: the Non-IC organization must be approved by the IC CHCO to have the vacancy posted, next an IC-civilian applies and is selected, and lastly a Memorandum of Understanding (MOU) is created and finalized. The Non-IC vacancy must follow IC JDA vacancy requirements, to include: generally reimbursable, 12 to 24 months in duration, open to GS-11 (or equivalent) and above, and published for a minimum of 15 days. The Non-IC organization should work with the IC Joint Duty Program Office to submit the vacancy and have it posted on JDAT. For more information or to advertise your Non-IC JDA vacancy, please contact the Joint Duty Program Office at ***icjointduty@dni.gov***.

Federal Partner Quarterly Counterintelligence & Security Roundtable

Elizabeth H, Federal Partners Group, NCSC/MID

On Wednesday, November 4th, 2020, the Federal Partners Group (FPG) held a quarterly virtual Federal Partner Counterintelligence and Security Roundtable pertaining to Chinese Recruitment. Attendees included multiple Non-title 50 federal partner agency representatives as part of ongoing information sharing efforts. The two guest speakers, both from academia, briefed federal partners at the Unclassified level. Joseph O'Neill, from the National Intelligence University, provided a presentation entitled "China's 'Traditional' Human Intelligence Collection." Additionally, Ken Wisian, Ph.D., delivered a presentation entitled "Working with Chinese Academics, Students and Funders, a Perspective." Representatives from 20 federal partner departments and agencies dialed in with over 80 participants.

National Insider Threat Task Force Hub Courses

Robert L, National Insider Threat Task Force, NCSC

The National Insider Threat Task Force (NITTF) issued a directive on Insider Threat Awareness Training for federal agencies to use the Defense Counterintelligence and Security Agency (DCSA) Center for Development of Security Excellence (CDSE) web-based Insider Threat Awareness course. This course, and others, can be found at the following website:

https://securityawareness.usalearning.gov.

The DCSA CDSE site is available to all government Departments and Agencies (D/A), and certificates are available after course completion. Additional DCSA CDSE training can be found at ***http://www.cdse.edu/catalog/insider-threat.html***.

The NITTF is hosting virtual Insider Threat Hub Operations courses throughout 2021. The Insider Threat Hub Operations course introduces and exercises the basic functions of an insider threat program's centrally managed analysis and response capability (aka Hub) 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.

When: All courses are held from 8:00am – 4:30pm. Below are the HUB courses scheduled for 2021 along with the date registration opens for each course.

January 26-27, 2021 (Opens December 1, 2020)

February 23-24, 2021 (Opens January 1, 2021)

April 13-14, 2021 (Opens March 1, 2021)

May 18-19, 2021 (Opens April 1, 2021)

June 22-23, 2021 (Opens May 3, 2021)

August 10-11, 2021 (Opens July 1, 2021)

September 14-15, 2021 (Opens August 2, 2021)

October 19-20, 2021 (Opens September 1, 2021)

Location: Online via CISCO WEBEX

Audience: Government employees supporting an executive brand department's or agency's insider threat program.

Cost: No cost

Register: Email ***NITTF_Training@dni.gov*** with participant(s) name, email address, and agency. For more information, go to ***https://www.dni.gov/index.pho/ncsc-how-we-work/ncsc-nittf***.

> *"This course introduces and exercises the basic functions of an insider threat program's centrally managed analysis and response capability…"*

Mitigating Risk to USG Employees In Critical HUMINT Threat Countries

Michael Carr, Special Agent, U.S. Department of State, Diplomatic Security Service, Office of Counterintelligence

At any given time, more than 10,000 U.S. Government (USG) employees from more than 20 Executive Branch agencies are assigned to any one of 275 diplomatic missions abroad under Chief of Mission (COM) authority. In a select number of countries designated as a Critical HUMINT threat on the State Department's Security Environment Threat List, USG employees face an unprecedented and aggressive level of targeting by Foreign Intelligence Entities (FIE) due to the political sensitivity of these posts. To counter this threat, a program of enhanced counterintelligence vetting was established by the Overseas Security Policy Board (OSPB) to evaluate suitability for assignment in these environments.

The OSPB has established a baseline level of mandatory vetting that all Executive Branch agencies must follow to screen employees proposed for assignment to a Critical HUMINT threat country under COM authority. Known as the Pass-Through program, this vetting evaluates employee risk of exploitation by FIE through review of the employee's background against 13 criteria set forth in the Foreign Affairs Handbook, 12-FAH-6 H-211.5. These criteria represent vulnerabilities that have been historically leveraged by FIE in Critical HUMINT threat countries when targeting USG employees.

If an employee's background meets any of the criteria in 12-FAH-6 H-211.5, a determination of suitability for assignment must be made by the parent agency in consultation with the Diplomatic Security Service, Office of Counterintelligence. Executive Branch agencies that have official representation in Critical HUMINT threat countries are encouraged to contact the Diplomatic Security Service, Office of Counterintelligence for guidance on Pass-Through program development, training, and support.

Chinese Recruitment and Collection Efforts

Counterintelligence Mission Center, CIA

Any American can become a target of Chinese security services. China is one of the most hostile counter-intelligence threats Americans are facing today. Chinese intelligence services target a range of persons globally, including individuals not of Chinese ethnicity, who have access to sensitive information or have the potential to gain access. China's success in recruiting Western businesspeople is in part due to its use of incentives to encourage cooperation. China is increasingly offering large sums of money for information, all-expense paid trips to China, and assistance in developing access to the lucrative Chinese business market or meetings with influential clients. While China often relies on economic incentives to lure Western businesspeople, the services also have used aggressive, coercive methods such as blackmail and sexual entrapment.

The following are three core missions that drive Chinese recruitment and collection efforts:

- The core mission of the Chinese security services is to protect the Chinese Communist Party (CCP) from regime threats. The services will therefore focus particular attention on Americans who associate with persons or groups that Beijing considers to be "dissident" or a threat to internal stability.
- Another key mission of the security services is to collect strategic foreign intelligence on the US. They are trying to gather sensitive political, economic, and military data on the US, to learn about our plans and intentions for the trade war and other key bilateral issues.
- Finally, China takes a whole-of-government approach to acquiring advanced Western technology, from legal acquisition methods to the outright theft of trade secrets. Its intelligence services are actively involved in identifying and recruiting US businesspersons who can steal proprietary data and bring it back to China. The goal of China's technology acquisition is not only to indigenize production and reduce China's dependence on Western supply chains. It is also to position Chinese companies to become global leaders in these industries. In some cases, China's theft of trade secrets has inflicted significant economic damage to US businesses.

LINKING TO NCSC

"The Nevernight Connection" - ***https://youtu.be/N5V7G9IBomQ***

FBI Counterintelligence Resources - ***www.fbi.gov/nevernight***

NCSC Counterintelligence Resources - ***https://www.dni.gov/index.php/ncsc-features/2780***

NCSC/FBI Press Release - ***https://www.dni.gov/files/NCSC/documents/features/20200929-Press-Release-on-Nevernight-Connection.pdf***

U.K. CPNI "Think Before You Link" - ***https://www.cpni.gov.uk/security-campaigns/think-you-link***

U.K. CPNI "Glitch" - ***https://www.cpni.gov.uk/system/files/campaign_assets/Glitch%20with%20TEXT%20and%20music%203_0.mp4***

From the Director

William R. Evanina
NCSC Director

The National Counterintelligence and Security Center (NCSC) and FBI recently released a movie --"The Nevernight Connection" -- to raise awareness of how foreign intelligence services and other hostile actors increasingly use fake profiles on social media platforms to target Americans for recruitment and information gathering. This is a threat that every U.S. government employee needs to be aware of.

Posing as headhunters or consultants on professional networking sites and other social media platforms, hostile foreign actors are aggressively targeting individuals across the U.S. government, as well as in business and academic communities, to obtain valuable and sensitive information. Don't fall for these malicious online approaches.

Watch "The Nevernight Connection" and check out the NCSC/ FBI press release to understand the risks involved and how to guard against this threat. Additional resources and information from the FBI and NCSC can be found online. Earlier this year, the U.K. Centre for the Protection of National Infrastructure (CPNI) also released information to help U.K. industry and government sectors address this threat.

> *"This is a threat that every U.S. government employee needs to be aware of."*

Social media deception continues to be a popular technique for foreign intelligence services to glean valuable information from unsuspecting Americans, including federal employees and contractors. Through this movie and other resources, we hope to raise awareness among Americans so they can guard against online approaches from unknown parties that could put them, their organization and even national security at risk.

We hope you're finding these Newsletters useful. If you have any suggestions, articles you would like to submit, or other thoughts on how we can enhance our engagement with federal partners, please let us know at ***NCSC_FEDS@dni.gov.*** For more information on NCSC and counterintelligence and security topics, including the supply chain, please visit our website at ***https://www.NCSC.gov*** or follow us ***@NCSCgov on Twitter.***

William Evanina