Federal Partner Newsletter

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

Volume 2 | Issue 2
September 2020

FY 2019 National Defense Authorization Act (NDAA) Section 889

Jeanette M, Supply Chain & Cyber Directorate, NCSC

The National Counterintelligence and Security Center (NCSC) has been working in conjunction with the Office of Management and Budget (OMB) and the Federal Acquisition Security Council to provide supply chain security guidance to federal agencies. Specifically, this guidance was developed as federal agencies began to fully implement Section 889 of the NDAA for FY2019, which prohibits federal agencies from contracting, directly or indirectly, with five Chinese firms and their subsidiaries: Huawei, ZTE Corporation, Hyteria Communications, Hanghzou Hikvision and Dahua Technology Company. The broader provision of Section 889 prohibits federal agencies from contracting with any company that uses goods and services from these five Chinese firms, unless a federal agency authorizes a waiver for a specific company, which can only be granted by the agency head after receiving NCSC supply chain security guidance. In addition to the guidance documents, available on the OMB Max page, NCSC arranged to provide updated classified briefings on the supply chain threats and third party risks stemming from contracting with companies that have these five firms in their corporate supply chains. These contracting prohibitions support a key objective of the National Counterintelligence Strategy of the United States 2020-2022, namely, to reduce threats to key U.S. supply chains. NCSC stands ready to provide supply chain security guidance to federal agencies as they continue to elevate supply chain security in the acquisition process.

Nuclear Regulatory Commission (NRC)

Advising its Workforce to be Vigilant

Lance English, Counterintelligence Program Manager, U.S. Nuclear Regulatory Commission

The NRC prepared an announcement for its workforce, reminding them to be vigilant regarding possible exploitation of virtual domestic and international meetings by foreign intelligence services (FIS) and potential for online elicitation. Here is an excerpt from the announcement:

FIS are often highly motivated to obtain the information they seek, and the widespread use of virtual meeting and conferencing platforms amid the Coronavirus public health emergency has created more opportunities for illicit online activity. As the NRC continues to carry out its critical safety and security mission in this new environment, please review the following tips for mitigating the threat:

> Virtual meetings make it difficult to verify the identity of participants, particularly when interfacing with new contacts, as is often the case in international fora. FIS may leverage virtual meetings as cover for espionage-related activities by impersonating established contacts. Online meetings could also be used to support targeted cyber operations to gain or expand access to NRC's networks. Surreptitious cyber operations enabled through virtual meeting platforms could be used to gain access to sensitive and/or proprietary information. Exploitation of these meetings may further allow FIS access to your email, chats, contacts, and scientific data not available publicly.

- Be mindful of the information you share while conducting virtual meetings, both personal and work-related.
- Be aware that information shared during virtual meetings can be used as blackmail to place employees in compromising positions, or to spot potential targets.
- Be mindful that some virtual meeting and collaboration platforms are foreign-owned and may be subject to a range of intelligence and privacy laws that differ from those in the United States. Some foreign national security laws require your data to be stored on or pass through foreign servers, and foreign governments may even require direct or on-demand access to this data unbeknownst to you or other participants.
- Maintain awareness of agency announcements and guidance for current information on vulnerabilities associated with commonly-used virtual platforms (e.g., the Office of the Chief Information Officer's April 2020 announcement regarding the Zoom conferencing application).
- Avoid downloading and installing meeting-based applications on your devices; use web-based tools instead.
- Be mindful of sudden changes to the list of meeting attendees, particularly drastic changes to the participant list or last-minute additions.
- Know who is in attendance in virtual meeting space and be clear on what information is permitted to be discussed in advance of the meeting. Avoid discussions that "dance around" classified or sensitive information. Note that classified information is only permitted to be discussed in secure spaces using approved secure communication systems.

- FIS may mimic know contacts, so be sure to verify the requestor's identity before replying to messages or requests for information.
- Check for spelling errors in emails or links, and look-alike domains for conferencing sites or applications.
- When in doubt, report concerns to the appropriate NRC points of contact using the instructions below.

For additional information regarding counterintelligence concerns while conducting virtual meetings or using telework platforms, please reference the counterintelligence SharePoint site, or the National Counterintelligence and Security Center's website.

Insider Threat Awareness Month

Charles M, National Insider Threat Task Force

September is Insider Threat Awareness Month. The National Insider Threat Task Force is partnering with the Office of the Undersecretary of Defense for Intelligence and Security, the Department of Homeland Security, the Defense Counterintelligence and Security Agency and other Insider Threat community stakeholders to present the second National Insider Threat Awareness Month (NITAM) program in September 2020.

When: Thursday, September 3, 2020 from 10:00 am to 3:00 pm EDT

Audience: Insider Threat practitioners and Counterintelligence and Security practitioners from the Department of Defense, Federal Agencies, private industry, critical infrastructure sectors, and academia

Where: Register for the virtual conference at https://www.cdse.edu/itawareness/index.html

Classification: The conference is UNCLASSIFIED.

For information about the NITAM 2020 Virtual Conference see https://cdse-events.acms.com/content/connect/cl/7/en/events/event/shared/683576/event_landing.html?sco-id=6819559.

Safeguarding Our Future

Kenneth P, National Counterintelligence Directorate, NCSC

NCSC provides unclassified one-page *Safeguarding Our Future* bulletins. Each bulletin provides a brief overview of a specific foreign intelligence threat, as well as impacts of the threat and steps for mitigation. You can find these awareness materials at https://www.dni.gov/index.php/ncsc-features/2762.

Looking forward, NCSC will publish a new line entitled *Safeguarding Our Elections*.

SAGE Collaboration Tool

Vera S, Mission Integration Directorate, NCSC

The Federal Partners Group is in the process of establishing a collaboration page on the Structured Analytic Gateway for Expertise (SAGE). The Office of the Director of National Intelligence launched in SAGE in 2011. This website provides a secure unclassified forum for collaboration amongst all levels of government, academia, and private sector industry partners. It includes public and private spaces. Some of the features include uploading and sharing of documents, discussion posts, blogs, polls, event announcements, and streaming RSS feeds. It is approved for use up to the Unclassified/For Official Use Only level, and it is accessible via personal electronic devices. Federal Partner Primary and Alternate contacts will receive an invitation to join the group. If you do not receive an invitation by September 30, 2020 or would like to invite other personnel to the Federal Partners Group on SAGE, please contact Vera S at verals2@dni.gov.

FPG Activity Updates

Vera S, Mission Integration Directorate, NCSC

Due to the COVID-19 pandemic, the NCSC Federal Partners Group canceled the Federal Partners Forum scheduled for May 2020 and the Quarterly Roundtable scheduled for July 2020. We intend to resume our information sharing activities and are planning new events that will likely be virtual. Our first event is a Roundtable update planned for September 2020. We are interested in your input, needs and interests for these activities. Please provide your ideas and comments to Vera S at verals2@dni.gov or William G at willieg1@dni.gov.

LINKING TO NCSC:

Supply Chain Briefs - https://www.dni.gov/index.php/ncsc-newsroom/item/2141-ncsc-briefs-agencies-across-the-u-s-government-on-supply-chain-threats-posed-by-five-specified-chinese-companies

July 2020 Election Threat Update - https://www.dni.gov/index.php/ncsc-newsroom/item/2140-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public

2018 Foreign Economic Espionage in Cyberspace Report - https://www.dni.gov/index.php/ncsc-newsroom/item/1889-2018-foreign-economic-espionage-in-cyberspace

National Counterintelligence and Security Strategic Plan for 2018 – 2022 -https://www.dni.gov/files/NCSC/documents/Regulations/2018-2022-NCSC-Strategic-Plan.pdf

NCSC Awareness Materials - https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-know-the-risk-raise-your-shield/ncsc-awareness-materials

Wall of Spies - https://www.intelligence.gov/wall-of-spies

From the Director

William R. Evanina
NCSC Director

Thinking about the unprecedented challenges we continue to face this year, I am reminded of the words of President Abraham Lincoln—"Be sure to put your feet in the right place, then stand firm."

Each of us plays a vital role in safeguarding America against our adversaries by promoting united and integrated counterintelligence and security communities. These communities depend on us, their individual practitioners, to put our feet in the right place by maintaining the highest standards of personal and professional conduct. We stand firm when everyone in these communities—federal, state, local, tribal, private sector, academic, research—effectively collaborates and cooperates.

As Federal Partners, your efforts in these vital mission spaces are integral to our nation's security. Our adversaries have repeatedly demonstrated their voracious appetite for information from all corners of the federal government as well as the private sector. Your organizations and the information they generate are frequent targets. We must work together to deny adversaries the information they seek.

Although the global COVID-19 pandemic has forced our communities to approach our missions with the utmost flexibility, it is clear to me that we are rising to meet the challenges. We have adjusted and found new ways to carry out our counterintelligence and security responsibilities, while continuing to meet our high standards. The forward momentum of these efforts must continue.

The National Counterintelligence and Security Center (NCSC) remains a resource that each of you may call upon for support and assistance. NCSC is focused on helping you achieve success. We hope you find this newsletter to be a valuable source of information and another way for us to remain connected. If you have any suggestions, articles you would like to submit, or other thoughts on how we can enhance our engagements with you, please let us know at NSCS_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

"As Federal Partners, your efforts in these vital mission spaces are integral to our country's continued safety from those groups and nations that oppose us and seek to do us harm."