Federal Partner Newsletter

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

Volume 1 | Issue 3
October 2019

Intelligence Community Security Coordination Center

Aram S., Supply Chain & Cyber Directorate (SCD), NCSC

The IC Security Coordination Center (IC SCC) is the only one of seven Federal Cyber Centers that integrates actionable CI, security and insider threat information with cybersecurity vulnerability data. It serves as the Federal Cyber Center for the integrated defense of the IC Information Environment (IC IE) and the IC Information Technology Enterprise (IC ITE) on behalf of the DNI and IC CIO.

The IC SCC is actively involved in expanding the sharing of IC cyber indicators to improve cybersecurity across the U.S. government and critical infrastructure. It is the service provider for information security services in support of the IC ITE. IC SCC provides tools and services that facilitate situational awareness during steady state operations, and coordinates the integrated community response for the IC IE during significant cyber events.

The IC SCC is led in a partnership among the NCSC, IC CIO & DIA. The Supply Chain and Cyber Directorate (SCD) of NCSC provides one of the Deputy Directors of the IC SCC—the Deputy Director for Counterintelligence. The ODNI IC CIO provides the IC SCC Director and DIA provides the Deputy Director for Cyber. A Technical Deputy Director position is also filled by the IC CIO.

The graphic below illustrates the areas of responsibility for the main information domains covered by the Federal Cyber Centers. IC SCC is responsible for managing the threat and asset response for the IC Information Environment, the TS/SCI domain of the IC elements and NT-50s. United States Cyber Command (USCYBERCOM) is responsible for managing the threat and asset response for the Department of Defense Information Network (DODIN). DHS's National Cybersecurity and Communications Integration Center (NCCIC) is the focal point for managing the national response efforts for significant cyber events for activities within the scope of DHS authorities.

Health & Human Services (HHS)

Protecting Americans

Now and Beyond

Michael Schmoyer, PhD, National Security Advisor to the Secretary, U.S. Department of Health & Human Services

The U.S. Department of Health & Human Services (HHS) seeks to protect, promote, and advance the health of Americans worldwide every day. HHS does that by providing for effective health and human services and fostering advances in medicine, public health, and social services. And since Secretary Shalala first designated HHS as a National Security Department in 1995, HHS has focused on protecting Americans on the physical plane as well as the cyber domain.

The President's Fiscal Year (FY) 2020 Budget supports HHS' mission by prioritizing key investments that work towards fulfilling the Administration's commitments to improve American health care, address the opioid crisis, lower the cost of drugs, and streamline federal programs to better serve and safeguard the American people. The FY20 budget proposed $87.1 billion in discretionary budget authority and $1.2 trillion in mandatory funding for HHS. Furthermore, with this level of funding and programmatic responsibility, HHS has developed significant protective capabilities across the Department as it relates to addressing the strategic threat of cyber economic espionage, safeguarding from foreign intelligence services, and looking at emerging threats in the cyber domain, such as supply chain risk management.

For example, the Office of National Security (ONS, the Federal Intelligence Coordination Office for HHS) works with partners throughout the Department to maintain defensive programs to prevent intelligence

collection seeking to obtain HHS technology, intellectual property, trade secrets and proprietary information. These areas alone have had ONS working with partners across the Intelligence Community, the National Security Council, the Office of Science Technology Policy, Congress, and Institutes of Higher Education extensively over the past three years. We have only seen the collaboration, cooperation, and communication expand as those relationships continue to develop.

ONS is excited about FY20! We will embrace expanded partnerships with our internal cyber partners, further support of the Committee for Foreign Investment in the United States, and establishing formal policy within the Department relating to supply chain risk management. We will continue to leverage our relationships across the Intelligence Community and especially look forward to continued support from NCSC's Federal Partner's Group

Did You Know? **1)** 33% of the U.S. GNP is related to healthcare.

2) HHS has a uniformed service of more than 6,000 health professionals with the Surgeon General as the head of the Commissioned Corps.

Defensive Counterintelligence Framework (DCIF)

Manuel L., Federal Partner Group, Tiger Team

What is the Defensive Counterintelligence Framework (DCIF), and how can you use it to help your department/agency's counterintelligence (CI) program? The DCIF is a NCSC-developed primary diagnostic tool that can be used to help evaluate your current CI program efforts in two ways: as a self-evaluation tool, or as a diagnostic tool that informs a deeper engagement with NCSC's Federal Partners Group's Tiger Team.

The DCIF is a compilation of 54 questions across seven CI program domains: Program Management, CI Analysis & Support to Operations, Cybersecurity, Information Sharing & Awareness, Infrastructure & Sensitive Asset Protection, Personnel Security & Foreign Vetting and Access, and Training. It addresses NCSC-identified "essential" program elements of an effective CI program, and responses to the questions help identify program gaps and highlight potential areas for improvement.

When paired with a Tiger Team engagement, your department/agency's DCIF responses inform the Team's inquiries, resulting in a more comprehensive NCSC-issued report, which is written in full consultation with your CI program leads. Federal Partners seeking an independent, objective evaluation of their CI program's efforts have found these reports to be essential in appealing to senior officials for resources and policies to address identified program gaps. In fact, previous engagements have had positive results to include the addition of numerous CI-designated billets within Federal Partner CI programs.

For more information on the DCIF and/or Tiger Team assistance in using the DCIF, please contact us at NCSC_FEDS@dni.gov .

UPCOMING EVENT: SCRM Workshop (Maintenance & Disposal)

Nov. 8, 2019, ICC-B, 1C-116, 0900-1200

From the Director

William R. Evanina
NCSC Director

October is national Cybersecurity Awareness Month, reinforcing for us all that cybersecurity is a shared responsibility affecting every American. The cyber threat landscape is evolving as our adversaries become more assertive and adept at using cyberspace to target America. In addition, the number of adversaries is growing as is the availability of malware, providing new actors with opportunities to launch malicious cyber operations.

The potential impact of these cyber operations is amplified by our increasing interconnectedness. The integration of technology, such as artificial intelligence and the Internet-of-Things, into our daily lives adds convenience, but also significant risk. New technologies introduce new vulnerabilities that the cybersecurity community must be prepared to defend.

We are all potential cyber targets, whether from criminals, terrorists, hacktivists or nation states. Future battles may be lost by individuals who don't have the proper awareness of cyber threats, and, therefore, enable the compromise of critical data and networks. For these reasons, we must all enhance our understanding of cyber threats and know what we can do to mitigate the risks. By being aware and practicing proper cyber hygiene, we can each do our part in making it much harder for our cyber adversaries.

> "The threat we face has never been greater. Cybersecurity has to be everyone's job."

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, please visit our website at **https://www.*NCSC.gov*** or follow us ***@NCSCgov on Twitter.***