Federal Partner Newsletter

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

Volume 2 | Issue 1
January 2020

Continuous Evaluation Program — Update

Valerie K., Special Security Directorate, NCSC

The number of security clearance holders enrolled in the ODNI Continuous Evaluation System (CES) for automated records checks passed the quarter-million mark, and the enrolled population now exceeds 330,000. To highlight the significance of this milestone, the CES enrolled population in November 2018 was approximately 29,000. The CES enrolled population is comprised of federal civilian, contractor, and military employees from 29 Executive branch agencies and enrollment continues to grow.

ODNI's CES technical capability is a cornerstone of security clearance modernization efforts to reduce the inventory of personnel security background investigations, increase the timeliness and frequency of Information reviewed between reinvestigation cycles, and help maintain a trusted workforce. As the Executive Branch moves toward a Continuous Vetting framework under the Trusted Workforce 2.0 initiative, we anticipate continued enrollment in the ODNI CES.

UPCOMING EVENTS:

25-27 February—NITTF Hub Ops Course, Centra (all day)

16 April—FBI-hosted 811 Referral Conference (FBI HQ) 0830-1600

22-23 April—6th National Supply Chain Workshop (SCOR)

28-30 April—Annual OPSEC Symposium, Maritime Conference Center

30 April-1May—SCRM Workshop at ICC-B

Federal Partner Quarterly Counterintelligence & Security Roundtable

Vera S., Federal Partners Group, NCSC/MID

The Federal Partners Group (FPG) held its Federal Partner Quarterly Counterintelligence and Security Roundtable on January 29. The theme for the meeting was economic espionage and featured briefings from the National Counterintelligence Officer for East Asia on" Beyond Espionage: Protecting Research Infrastructure," and the Chief, Counterintelligence and Export Control Section, National Security Division, Department of Justice on legal aspects of economic espionage and theft of trade secrets. These briefings addressed the threat to the U.S. economy posed by China's science and technology strategy. Takeaways included the need for a forum for engaging with regulators on counterintelligence, and the desire for a coordinated strategy on industry outreach.

Did You Know?

- NOAA Commissioned Officer Corps is the smallest of the uniformed services with only 370 officers.
- Selective Service System manages the third largest personally identifiable information (PII) database in the federal government.

Insider Threat— A U.S. International Development Finance Corporation's (DFC's) Perspective

John Abreu, Senior Policy Advisor, National Security Division, Department of Justice

Even though all insider threat programs must build in accordance with the minimum standards, a successful insider threat program is not a one size fits all, and must adhere to two major staples: mission integration and integration of organizational culture. This is to say that a program must find a proactive way to assist the organization with fulfilling the mission, become a value added, and not a roadblock.

To ensure that the Insider Threat program is integrated successfully with mission, the program should be able to answer the following questions – what is my organization's mission, and how does my program proactively support it? One approach to take is using foreign travel threat briefings to ensure that organizational employees are equipped with knowledge that can reduce or mitigate the potential of becoming victims of crime, or a target of a foreign intelligence service.

The next major staple that determines the success of the program is how well the program is integrated into the culture of an organization. A Department of Defense organization, Non-Title-50 (NT-50) Department or Agency (D/A), or Intelligence Community (IC) element will more than likely have different organizational cultures; and therefore, their respective Insider Threat programs should reflect their respective cultures. If an insider Threat program within a NT-50 D/A uses language or even case studies from an IC element, it may find that its program never gains traction with their employees, which will lead to less reporting and the potential for the program to become irrelevant. This does not negate the fact that Insider Threat programs across the government can learn from one another, rather it points to the need to adapt the program to meet respective organizational cultures.

In summary, an organization's mission should dictate the "why" of your Insider Threat program, and the organization's culture should dictate the "how."

From the Director

A core mission of the ODNI's National Counterintelligence & Security Center (NCSC) is to provide the private sector, academic, and research communities with information about foreign intelligence threats to their organizations and share best practices for mitigating risks. The goal is to make these sectors harder targets so they understand the threats, anticipate them, and can take steps to guard against them.

"It's incredibly important that we take information about threats to the private sector and academia and get it into the hands of those vulnerable to attack," said NCSC Director William Evanina. "These communities are squarely in the cross-hairs of well-financed, nation-state adversaries and need our support and assistance."

In fulfilling that mission, NCSC has engaged in an extensive effort over the past two years to raise awareness in industry and academia about the foreign intelligence threats such as the Chinese government's systemic campaign to siphon technology, research, and innovation from America's open economic and academic systems. Working with partners across the U.S. government, NCSC has provided insights into the Chinese government's ambitions, capabilities, and tactics, and how they adversely impact U.S. economic and national security.

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.***

William Evanina