

**STATEMENT BY NCSC DIRECTOR WILLIAM EVANINA  
FOR THE HOUSE COMMITTEE ON OVERSIGHT  
AND GOVERNMENT REFORM  
SUBCOMMITTEE ON GOVERNMENT OPERATIONS HEARING ON  
“SECURITY CLEARANCE INVESTIGATION CHALLENGES AND  
REFORMS”**

*Wednesday, 11 October 2017  
Room 2154 Rayburn House Office Building  
2:00 p.m.*

Chairman Meadows, Ranking Member Connolly, and Committee Members, thank you for the opportunity to appear before you today to discuss security clearance investigation challenges and reforms.

As the Director of the National Counterintelligence and Security Center (NCSC), I am responsible for leading and supporting the counterintelligence and security activities of the U.S. Government, including the U.S. Intelligence Community.

The Director of National Intelligence (DNI) is designated as the Security Executive Agent (SecEA). In this role, the DNI is responsible for the development, implementation, and oversight of effective, efficient, and uniform policies and procedures governing the conduct of investigations, adjudications, and, as applicable, polygraphs for eligibility for access to classified information. The NCSC has been designated as the lead staff support element to enable the fulfillment of the DNI’s SecEA responsibilities.

We are responsible for the oversight of policies governing the conduct of investigations and adjudications for approximately 4.1 million national security cleared personnel. The security clearance process includes determining if an individual is suitable to receive a security clearance, conducting a background investigation, reviewing investigation results, determining if the individual is eligible for access to classified information or eligible to hold a sensitive position, facilitating reciprocity, and periodically reviewing the individual’s continued eligibility.

As NCSC exercises the SecEA responsibilities, it works closely with the agencies responsible for actually conducting the investigations and adjudications, and managing other security programs associated with clearances. This ensures

that our policies and practices are informed by those working to protect our personnel and sensitive information. One of those agencies is the National Background Investigations Bureau (NBIB); and its Director, Charlie Phalen, is also here today, along with Garry Reid, Director for Defense Intelligence (Intelligence and Security), Department of Defense.

In addition to supporting the DNI in his role as SecEA, one of my other responsibilities is to support the DNI and Attorney General's efforts to ensure that departments and agencies across the federal government have Insider Threat programs established to help deter, detect, and mitigate the actions of individuals who may have the intent to unlawfully disclose classified information or possibly do harm to themselves or others. The Insider Threat programs go beyond traditional personnel security practices implemented upon hiring, and offer an ongoing, holistic approach to ensuring the well-being of the cleared workforce. These programs help us to be more proactive in preventing unauthorized disclosure, by minimizing potential security gaps and/or identifying personnel who need assistance, and getting them help before any damage occurs.

I believe the first step in identifying and preventing an insider threat is the initial, and periodic, background investigation. This application—and subsequent investigation—will continue with the clearance holder as a foundational assessment throughout the period of time the employee holds their security clearance. So the interrelationship between the security clearance process and insider threat detection is critical.

I am going to focus my remarks on the efforts to improve security clearance processes and procedures, reciprocity, as well as the general challenges we face, including the backlog of investigations.

NCSC is engaged in a transformation of the security clearance process, and remains committed to providing Departments and Agencies policy direction, while continuously assessing new ways for improvement. We have issued guidance to the community on a wide variety of issues, which we would be happy to provide to the Committee.

Additionally, we partner with the Director, Office of Personnel Management (OPM), who serves as the Suitability and Credentialing Executive Agent, to align the security clearance process for National Security, Suitability and Credentialing. The following achievements have resulted from this collaboration:

- Creation of the National Training Standards for Background Investigators, National Security Adjudicators, and Suitability Adjudicators, which align training requirements across National Security, Suitability and Credentialing.
- Issuance of the Federal Investigative Standards (FIS), which align investigative requirements for suitability and national security, building upon previous investigative work, and avoiding duplication, where possible.
- Provided clarifying guidance to the position designation process using the Position Designation Tool. The tool aids in the classification of national security positions regardless of a requirement for access to classified information (i.e. Law Enforcement Officers). As a result, Title 5 Code of Federal Regulation (CFR) Part 732, was reissued as 5 CFR Part 1400.

We have also implemented efforts to track and report on the application of security clearance reciprocity. Reciprocal acceptance of background investigations and National Security determinations support employee mobility and mission accomplishment, which is a critical element to ensure maximum effectiveness in human resource utilization. In FY 2016, the core IC agencies—the Central Intelligence Agency, the Defense Intelligence Agency, the National Geospatial Intelligence Agency, the National Reconnaissance Office, and the National Security Agency—reviewed and closed 35,130 requests and accepted (approved) 30,643 of these, for an acceptance (approval) rate of 87.2%. It took the core IC four days to apply the principles of reciprocity and accept the background investigation and security determination of another IC agency.

We are extensively engaged in modernizing security clearance processes in an effort that includes implementing Continuous Evaluation (CE) to conduct automated records checks on a segment of covered individuals between the five- and ten-year periodic reinvestigation cycles when security-relevant information may go unreported to security officials. CE is being implemented across the Executive Branch in phases, due to the anticipated increased workload demands, technical complexities associated with developing personnel security enhancements, and the unknown impact to agency workforce requirements.

Initial CE implementation began in October 2016, with a requirement for agencies to conduct automated records checks on clearance holders and on those eligible to hold a sensitive position (such as a border patrol officers), by 30 September 2017.

Metrics collected during implementation will be evaluated to assess how we can leverage CE to transform periodic reinvestigations. NCSC is also building an IT system that will conduct automated records checks, apply standard personnel security business rules, and generate alerts when security-relevant information is identified. Our goal is to deploy a fully operational CE System by Fall 2018 that will be available for use by any Executive Branch agency.

NCSC is also finalizing a plan to assist in the elimination of the backlog of periodic reinvestigations and implement the requirements directed by Congress in the Fiscal Year 2016 Omnibus Appropriation H.R. 2029 - 673 Enhanced Personnel Security Program (EPSP). The EPSP requires the DNI to direct Department and Agency heads to implement a program to provide an enhanced security review of covered individuals. No later than Fiscal Year 2021, the heads of the Agencies shall conduct automated records checks and check information from sources no less than two times every five years on the entire covered population, to ensure continued eligibility of each covered individual to access classified information and to hold a sensitive position.

As directed by Congress, the DNI, in coordination with interagency participation, will determine the feasibility of including additional data sources such as government, publicly available and commercial data, consumer reporting agencies, social media, and other sources.

The periodic reinvestigation backlog elimination plan uses a phased approach and specifically identifies NBIB's need to expand production capacity, implement process improvements, and stand up a modernized and secure IT architecture to eliminate its internal backlog of investigations. In response to the requirements of the Enhanced Personnel Security Program, we are working to incorporate capabilities developed through Continuous Evaluation to satisfy the EPSP requirement to periodically conduct records checks on all covered individuals.

Mr. Chairman, I defer to my colleague from NBIB to provide perspective on specific background investigation issues and challenges. I look forward to your questions.