UNCLASSIFIED STATEMENT FOR THE RECORD

ON SECURITY CLEARANCE REFORM

FOR THE

SUBCOMMITTEE ON OVERSIGHT OF GOVERNMENT MANAGEMENT, THE
FEDERAL WORKFORCE, AND THE DISTRICT OF COLUMBIA,

SENATE COMMITTEE ON HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS

MR. CHARLES B. SOWELL

DEPUTY ASSISTANT DIRECTOR FOR SPECIAL SECURITY, OFFICE OF THE
DIRECTOR OF NATIONAL INTELLIGENCE

JUNE 21, 2012

Introduction

Chairman Akaka, Ranking Member Johnson, distinguished Members of the Subcommittee: Thank you for this opportunity to discuss the progress we have made on security clearance reform. I am pleased to appear beside the principal partners of reform – the Department of Defense (DoD), the Office of Personnel Management (OPM) and the Office of Management and Budget (OMB) – who together work to ensure that improvements to timeliness, quality, and reciprocity are institutionalized and sustained.

Director Clapper continues to give extensive time and attention to this effort, and he recognizes that his role as Security Executive Agent (SecEA) is key to continuing the significant progress we have made in transforming the end-to-end security clearance process across the Federal Government. Clearance reform truly remains one of his top priorities.

We greatly appreciate the strong bipartisan support this initiative has received from this subcommittee, particularly Senator Akaka during your tenure as Chairman, and look forward to continuing our partnership with this committee and our fellow agencies across the Government to ensure further success.

Today I would like to focus my remarks on the Office of the Director of National Intelligence's (ODNI) efforts and accomplishments as the SecEA to implement comprehensive security clearance reform, highlight best practices in the Intelligence Community's (IC) clearance process that can be applied government-wide, and discuss some remaining challenges in standardizing policies and practices.

Accomplishments as the Security Executive Agent

Over the past two years, we have focused our efforts on institutionalizing the DNI's responsibilities as Security Executive Agent for the Government. In August 2011, we issued a policy clarification to eliminate discrepancies between intelligence community and national investigative standards, which immediately eliminated redundancy and improved government-wide reciprocity. In March 2012, the DNI issued Security Executive Agent Directive 1 (SEAD 1), a landmark publication, applicable US Government-wide, which provides a clear andcomprehensive description of the SecEA's authorities and responsibilities. SEAD 1 applies to all departments and agencies performing investigations or adjudications of persons proposed for eligibility to hold a sensitive position whether or not requiring access to classified information. The ODNI also led the inter-agency efforts to revise the National Security Adjudicative Guidelines which we expect to issue later this year.

Through his Security Executive Agent responsibilities, the DNI continues to support the Suitability and Security Clearance Performance Accountability Council's (PAC) goals of aligning security and suitability, and improving quality, timeliness and reciprocity. Our most mature oversight function is tracking and reporting security clearance timeliness data from agencies across the Government. Based on this data, the DNI began issuing annual letters in 2009 to departments and agencies not meeting the timeliness goals required by IRTPA for initial clearances. Over the past year we have refined our annual letters and added periodic reinvestigation timeliness and backlog numbers to assist agencies to focusing on those critical areas.

In January 2012, the DNI sent letters to 46 departments and agencies addressing their 2011 performance. Twenty-two agencies met the timeliness goals for all of 2011, nineteen agencies met the goals for some of the year, and only five agencies did not meet the goals and were directed to provide improvement plans. Of particular note, four of the five agencies which did not meet the goals in 2011 actually improved their performance throughout the year which demonstrated their commitment and progress. The military services, the Departments of Commerce, Energy, State, Transportation, Treasury and Veterans Affairs, OPM, Federal Bureau of Investigation, and National Security Agency are among the organizations that met the goals for all of 2011. I also want to highlight the Defense Security Service's Defense Industrial Security Clearance Office (DISCO), which met its timeliness goals for industry for the first time ever in 2011 and has continued to meet the goals for the past year.

DISCO's improved performance is tied to DoD's automated Case Adjudication Tracking System (CATS) which electronically adjudicates clean cases at the Secret level. This award-winning tool is a great example of DoD's powerful innovative capabilities to use automation for a more efficient allocation of adjudicative resources. DoD's efforts to share its automated adjudicative capability with other government agencies demonstrates government partnering at its best.

The dedicated oversight and assessment from this committee, the Government Accountability Office, the Security and Suitability Executive Agents, the PAC and the individual agencies and departments have combined to dramatically improve the government-wide average for initial clearances from 265 days in 2005 to 46 days in the

second quarter of FY 2012. We believe this is a clear demonstration of the power of partnership.

In addition to his oversight role, the DNI believes we must be responsive to department and agency emerging requirements and constrained resources. We hold quarterly Security Executive Agent Advisory Committee meetings with representatives from across the Government where we share ideas, best practices, and update each other on key policy, technology and training initiatives. We rotate these meetings throughout the Washington area with individual agencies hosting them. Past hosts include the State Department and Defense Security Service, and the Central Intelligence Agency is hosting our next meeting later this month.

Several agencies have approached the SecEA for guidance on using publicly available social media in the background investigation process. We have formed a working group to explore this issue and provide recommendations that will protect privacy and civil liberties while allowing the use of this emerging source of data; a SecEA Directive has also been drafted for coordination throughout the community. We have formed a working group to establish national level reporting requirements for individuals who are eligible or granted access to classified information. Working with our partners throughout both the IC and all of Government, we will standardize the way people report issues like foreign travel.

OPM is a critical partner, as the Suitability Executive Agent and largest investigative services provider for the Government. In August 2010, the ODNI and OPM jointly issued policy guidance which aligned suitability determination and security clearance investigation levels, essentially establishing reciprocity among them. The

ODNI and OPM have co-chaired the inter-agency Federal Investigative Standards (FIS) Working Group, tasked with revision of the FIS to align security and suitability investigations. Last month OPM and ODNI partnered to establish the FIS Implementation Working Group (FISIWG) that includes participation by all federal agencies with investigative authority. The FISIWG will collaboratively develop a high-level project plan, implementation strategy and timelines, deliverables and follow-on activities required for phased implementation of the revised Standards across the Federal Government. We are working with OPM to revise Background Investigator Training Standards to standardize training for background investigations, as well as Security and Suitability Adjudicator Training Standards. These training programs have been endorsed by the Performance Accountability Council. In the future, OPM and the ODNI will conduct joint assessments of agencies with suitability and security clearance investigation and adjudication authority. Our strong partnership will help us implement the reformed security clearance process and continue to make further improvements.

There is still work to do. We continue to focus on ensuring reciprocal acceptance of existing security clearances between agencies. To that end, we have put in place a reciprocity web page hosted on the SecEA Website that provides education and awareness, a checklist of exceptions, policy references, and examples of non-reciprocity issues. Another reciprocity initiative is the effort to document all DoD collateral clearances in Scattered Castles (SC); further, SC now includes fields that better support reciprocity. Measuring reciprocity is difficult, and despite an abundance of anecdotes, real data is hard to come by. To address this problem, we are developing a web-based form for individuals to submit their experience with reciprocity issues to the ODNI. This

will allow us, for the first time to collect empirical data, perform systemic trend analysis, and assist agencies with achieving workable solutions.

We have partnered with numerous industry associations to identify and address long-standing reciprocity issues. Industry is uniquely affected by reciprocity problems, and they have provided key insight to understanding the potential impact of a variety of SecEA efforts to make improvements. The ODNI is also a member of the National Industry Security Program Policy Advisory Committee (NISPPAC) and we have recently briefed our fellow members on the reciprocity website and web-based form initiative.

Best Practices in the IC Applicable Government-wide

One of the best practices in the IC security clearance process that can be applied government-wide is the continuous monitoring of cleared personnel, such as the program that NSA has implemented. Personnel security and CI professionals from NSA collaborate on initiatives to improve the timely detection of potential insider threats. Automated record checks are used to make re-evaluations more cost-effective, reduce adverse impact on agency resources and facilitate agency monitoring of employee conduct between standard reinvestigation cycles. Potential CI threats or associations are identified for further investigation.

As previously mentioned, the IC is exploring the use of social media in the clearance vetting process. An inter-agency working group is developing a recommendation to the SecEA for a government-wide social media policy and implementation strategy to use open source publically available electronic information to enhance security vetting, while respecting individual privacy and civil liberties. We are also reviewing data from government agencies and industry vendors suggesting potential

value in publically available electronic information on the internet. Several IC agencies are considering initiatives to conduct pilots involving checks of social media sites to determine cost-benefit. We expect to have a final recommendation to SecEA on government-wide applicability by December 2012.

<u>Challenges in Developing Standardized Policies and Procedures Relating to the Security Clearance Process</u>

Different formats of electronic and paper-based record systems at the federal, state and local levels, individual agency information protection policies and technology limitations pose some of the biggest challenges to improving further the security clearance process. To address these challenges, the PAC is re-establishing the Records Repository Working Group (RRWG) which will focus on improving information sharing and records exchange. In addition, the ODNI has formed a Data Standards Working Group (DSWG) with membership including all investigative service providers and agencies that conduct or adjudicate background investigations. The group is creating a standard by which all investigative data can be exchanged between organizations electronically. This achieves a number of purposes, including:

- Standardization of electronic data format and XML tagging of security background information

- Easy electronic transfer of data for reciprocity, reinvestigation, and adjudication

- Increased capability to use electronic adjudication

- Electronic (versus paper) storage of security "jackets"

- Reduction in the labor, time, and cost associated with rekeying and transporting physical files

In addition to benefiting the broader Government, as the IC moves ahead with its Information Technology Enterprise initiative, opportunities to leverage the work of the DSWG will abound.

Conclusion

Director Clapper is intent on creating a strong, effective Security Executive Agent capability for improvement of Government operations and efficiency. We hope the initiatives we have outlined demonstrate that.

Mr. Chairman, on behalf of Director Clapper, we appreciate your exceptional leadership on, and dedication to, security clearance reform. I hope our collective efforts and successes give you reassurance that time and energy you have devoted to this important national security capability has been very well spent. We look forward to continuing the partnership with our fellow agencies and this Subcommittee as we continue to strengthen our clearance processes in defense of the nation.