Office of the Inspector General of the Intelligence Community

(U) Audit Report of Intelligence Community Security Clearance Reciprocity

Report Number IC IG-AUD-2012-005

December 2012

Important Notice

This report contains information that the Office of the Inspector General of the Intelligence Community has determined is confidential, sensitive, or protected by Federal Law, including protection from public disclosure under the Freedom of Information Act (FOIA) 5 USC § 552. Recipients may not further disseminate this information without the express permission of the Office of the Inspector General of the Intelligence Community personnel. Accordingly, the use, dissemination, distribution or reproduction of this information to or by unauthorized or unintended recipients may be unlawful. Persons disclosing this information publicly or to others no having an officials need to know are subject to possible administrative, civil, and/or criminal penalties. This report should be safeguarded to prevent improper disclosure at all times. Authorized recipients who receive requests to release this report should refer the requestor to the Office of the Inspector General of the Intelligence Community.

(U) Table of Contents

(U) LIST OF TABLES

I. (U) EXECUTIVE SUMMARY

(U) WHY WE DID THIS AUDIT

(U) The Office of the Inspector General of the Intelligence Community (IC IG) conducted this audit in response to congressional direction in the Intelligence Authorization Act for Fiscal Year 2010. This audit examines whether there are policies and processes in place that facilitate timely reciprocity of personnel security clearances for (1) detailees and assignees; (2) Government employees transferring within the IC; and (3) contractors converting to Government positions.

(U) WHAT WE FOUND

(U) The Director of National Intelligence (DNI) issued policies to facilitate security clearance reciprocity and the mobility of IC personnel. As the Security Executive Agent, the DNI also is responsible for ensuring the recognition of security clearance reciprocity within the Executive Branch. The Special Security Directorate (SSD) within the Office of the Director of National Intelligence (ODNI) serves as the Security Executive Agent Executive Staff and executes those responsibilities within the Executive Branch and IC. While SSD recently completed what they consider to be foundational steps necessary to address security clearance reciprocity, the SSD has not yet established policies that identify standards for the length of time IC elements should take to process reciprocal security clearances; periodic reporting requirements for security clearance reciprocity; or the type of data that should be collected to facilitate security clearance reciprocity. We identified unreliable and unavailable data that we believe constrains the ability of the SSD to assess the extent to which IC elements honor security clearance reciprocity and calculate the time needed to process reciprocal security clearances. As a result, the SSD has limited ability to oversee and monitor whether IC elements are honoring security clearance reciprocity or processing reciprocal security clearances in a timely manner.

(U) The lack of an IC-wide policy that clearly describes when a *Questionnaire for National Security Positions,* or Standard Form 86 (SF-86), should be completed or updated by applicants who are eligible for security clearance reciprocity has led to different practices among IC elements. Requiring applicants who may be eligible for security clearance reciprocity to update an SF-86 as part of the hiring process can mitigate potential risks to national security that may have developed since the last investigation, but can also lengthen the processing time and reduce workforce mobility, which counters one of the the goals of security clearance reciprocity.

(U) The security clearance reciprocity determination is one piece of the IC hiring process. Human Resources processing and medical screenings also affect the overall length of time to complete the hiring process, even if the individual is eligible for security clearance reciprocity. Although those factors were outside the scope of our audit, we discuss them for informational purposes only.

(U) WHAT WE RECOMMEND

(U) The ODNI Assistant Director for SSD concurred with our recommendations to develop policies to ensure security clearance reciprocity is occurring in a timely manner and that IC elements follow consistent practices when requiring applicants to complete or update an SF-86.

II. (U) INTRODUCTION

(U) Since 1994, the United States Congress has expressed interest in improving security clearance practices and procedures, including government-wide security clearance reciprocity — that is all security clearances issued by authorized agencies across the U.S. Government would be accepted by all other agencies.[1] Congress has continually expressed concern that Federal agencies do not consistently honor previously granted security clearances and that Government employees and contractors who move or transfer among agencies experience delays in receiving clearance reciprocity or must undergo lengthy reinvestigations and adjudication by a new federal employer. As recently as June 2012, Congress identified the continuing need to ensure security clearance reciprocity is honored so that critical national security positions are quickly filled with the right people.

(U//~~FOUO)~~ Congress directed the Office of the Inspector General of the Intelligence Community (IC IG) in the Intelligence Authorization Act of FY 2010 to examine security clearance reciprocity within the Intelligence Community (IC).[2] This audit examines whether there were policies and procedures within the IC that facilitated timely reciprocity of personnel security clearances. Specifically, we assessed the time required to obtain a reciprocal security clearance for three categories of IC personnel:

1. an employee of an IC element who is detailed or assigned to another element of the IC (Detailees and assignees);
2. an employee of an element of the IC seeking permanent employment with another element of the IC (Government transfers); and
3. a contractor working within the IC who is seeking permanent employment with an element of the IC (Contractor conversions).

[1] (U) Hearing before the Senate Select Committee on Intelligence on the Joint Security Commission, 3 March 1994; *Open Hearing on Security Clearance Reform* before the House Permanent Select Committee on Intelligence, Subcommittee on Intelligence Community Management, 19 May 2009; *Open Hearing on Security Reform* before the House Permanent Select Committee on Intelligence, 1 October 2009; *Hearing on Security Clearance Reform* before the Senate Committee on Homeland Security and Government Affairs, Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, 16 November 2010; and *Security Clearance Reform: Sustaining Progress for the Future*, Hearing before the Senate Committee on Homeland Security and Government Affairs, Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, 21 June 2012.

[2] (U//~~FOUO)~~ Intelligence Authorization Act for Fiscal Year 2010, Pub. L 111-259. 124 Stat. 2654, Section 637(b), 7 October 2010.

(U) We encountered scope limitations that constrained our ability to assess the extent to which IC elements honor security clearance reciprocity and to calculate processing times. Those limitations include unreliable and unavailable data. Appendix C discusses those scope limitations in more detail.

(U) The time to process reciprocal security clearances alone does not communicate a complete picture of the time it takes to reassign or hire personnel into an IC element. We identified four other factors that affect hiring times that include: (1) internal processes for reassigning and transferring personnel; (2) determinations regarding an individual's eligibility for security clearance reciprocity; (3) human resources (HR) hiring processes; and (4) medical screening. However, those factors were outside the scope of our audit; consequently, we did not perform a comprehensive evaluation of all related policies and processes or their impact on processing times. We are providing those factors for informational purposes only, and we are not making any recommendations addressing those factors.

III. (U) BACKGROUND

(U) Congress passed section 3001 of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 to bring greater efficiency, speed, and interagency cooperation to the security clearance reciprocity process.[3] IRTPA requires all Federal agencies to accept security clearance background investigations (BIs) and access determinations completed by an authorized adjudicative or investigative agency. With the exception of polygraph examinations, IRTPA also prohibits agencies from establishing additional investigations or adjudicative requirements without the consent of the Director of National Intelligence (DNI) in his role as the Security Executive Agent.[4]

(U) Office of Management and Budget (OMB) Memoranda identify permitted exceptions to security clearance reciprocity.[5] Those exceptions remove the

[3] (U) United States House of Representatives Report 110-916, *Security Clearance Reform—Upgrading the Gateway to the National Security Community*, Nov. 20, 2008, and IRTPA, section 3001 (Pub. L 108-458, 118 Stat. 3707) 17 Dec. 2004.

[4] (U) *IRTPA* section 3001(d)(1)and (3)(A); Executive Order 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*, 30 June 2008.

[5] (U) OMB Memorandum for Deputies of Executive Departments and Agencies, *Reciprocal Recognition of Existing Personnel Security Clearances*, *Checklist of Permitted Exceptions to Reciprocity*, 12 Dec. 2005, revised 17 July 2006.

requirement for reciprocity and may require an individual to complete additional security-related processing actions before being cleared to work elsewhere within the Federal Government.

(U) Those exceptions include when:

- an individual does not meet polygraph requirements for a position;
- an existing clearance is an interim clearance;
- an individual is cleared at the Confidential or Secret level and the position for which they are being considered requires a Top Secret (TS) clearance;
- an investigation on which an existing TS/Sensitive Compartmented Information (SCI) access determination is based is more than 7 years old and, therefore, no longer considered to be in scope;
- the gaining agency has substantial information that surfaced since the last BI, indicating that the individual does not meet access eligibility standards or may no longer satisfy adjudicative requirements; or
- the existing access eligibility determination is subject to exceptions such as a waiver, deviation, or conditions.[6]

(U) Pursuant to Executive Order 13467, the DNI has served as the Security Executive Agent since June 2008. As the Security Executive Agent, the DNI is responsible for ensuring reciprocal recognition of eligibility for access to classified information among agencies throughout the Executive Branch and for arbitrating and resolving disputes among the agencies involving reciprocity of investigations and determinations of eligibility for access to classified information or eligibility to hold a sensitive position.[7]

[6] (U) OMB issued Memorandum for Deputies and Executive Departments and Agencies, *Reciprocal Recognition of Existing Personnel Security Clearances*, on 14 November 2007. The OMB memorandum defines exceptions, such as conditions, waivers, and deviations. An exception occurs when an agency head or designee grants or continues access eligibility to an individual despite the failure of the individual to meet adjudicative or investigative standards. A condition is when access eligibility is granted or continued with the provision that one or more mitigating measures are required, which may include additional security monitoring or restrictions on access to classified information. A deviation is when access eligibility is granted or continued despite a significant gap in coverage or scope of the BI, such as the lack of a name check or fingerprint check by the FBI. A waiver is when access eligibility is granted or continued despite the presence of substantial information that would normally preclude access. A waiver may require special limitations on access, additional security monitoring, or other restrictions on the individual's handling of classified information. The presence of an exception permits the gaining organization to reinvestigate or readjudicate the case prior to granting another security clearance.

[7] (U) Section 2.3(c), Executive Order 13467. *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*, 128 Fed. Reg. 38103, 30 June 2008.

(U) Security Executive Agent Directive-1, *Security Executive Agent Authorities and Responsibilities,* summarizes the authorities and responsibilities assigned to the DNI in the role as the Security Executive Agent.[8]

(U) The Security Executive Agent is responsible for the development, implementation, and oversight of effective, efficient, and uniform policies and procedures governing the conduct of investigations and adjudications for eligibility for access to classified information or eligibility to hold a sensitive position. The Security Executive Agent also is responsible for ensuring reciprocal recognition of eligibility for access to classified information, to include security clearance reciprocity among Federal agencies.

(U) Between 2008 and October 2012, the Security Executive Agent did not issue policies that govern security clearance reciprocity throughout the Federal Government. However, as head of the IC, the DNI issued several policies to facilitate security clearance reciprocity and the mobility of personnel in the IC.[9]

(U) Between 2007 and September 2010, the DNI delegated all authorities and responsibilities with respect to IC security policies to the Deputy Director of National Intelligence for Policy, Plans, and Requirements (DDNI/PPR).[10]
In 2008, the DDNI/PPR issued guidance for security clearance reciprocity within the IC that included:

- Intelligence Community Policy Guidance (ICPG) 704.1, *Personnel Security Investigative Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information,* which prohibits IC elements from conducting a reinvestigation unless a review of the *Questionnaire for National Security Positions,* or Standard Form 86 (SF-86) indicates that the person had a break in service of more than 24 months.[11]

[8] (U) Security Executive Agent Directive-1, *Security Executive Agent Authorities and Responsibilities*, 13 March 2012.

[9] (U) *National Security Act of 1947 as amended,* 50 U.S.C. §403-1 and section 1.3 (b), Executive Order 13470, *Further Amendments to Executive Order 12333*, *United States Intelligence Activities* 150 Fed. Reg. 45325, 4 August 2008.

[10] (U) ODNI Instruction No. 7007-3, *Delegation of Certain Authorities and Responsibilities of the Director of National Intelligence,* 21 June 2007.

[11] (U) The SF-86 *Questionnaire for National Security Positions* is a standardized form used by the Federal Government to collect information from applicants for national security positions. The information may be used as the basis for future investigations, security clearance determinations, and employment suitability determinations.

- ICPG 704.2, *Personnel Security Adjudicative Guidelines for Determining Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information,* which permits IC elements to review an updated SF-86 for individuals who have had a break in access of more than 60 days, the updated SF-86 indicates derogatory information since completion of the last SF-86, or if a polygraph interview is necessary.
- (U) ICPG 704.4, *Reciprocity of Personnel Security Clearance and Access Determinations*, established IC-wide direction to further define and coordinate security reciprocity among the IC elements. ICPG 704.4 requires the heads of IC elements to accept, without further security processing, all in-scope BIs and access determinations that are less than seven years old and have no exceptions to security standards.
- (U) ICPG 704.5, *Intelligence Community Personnel Security Database Scattered Castles*, mandates the recognition and use of Scattered Castles as the IC's authoritative repository for verifying personnel security access approvals regarding SCI and other controlled access programs and documents exceptions to personnel security standards. Each IC element uploads relevant information from its individual databases into Scattered Castles. Federal agencies outside of the IC store investigative and adjudicative information in either the Office of Personnel Management's Central Verification System or the Department of Defense's Joint Personnel Adjudication System.
- (U) Intelligence Community Standard Number 2008-700-1, *Glossary of Security Terms, Definitions, and Acronyms*, defines security clearance reciprocity as "the recognition and acceptance, without further processing, of security background investigations and clearance eligibility determinations." This Standard requires reciprocity when there are no waivers, conditions, or deviations to DNI security standards.
- (U) In 2009, the DNI issued Intelligence Community Directive (ICD) Number 709, *Reciprocity of Intelligence Community Employee Mobility,* to facilitate the movement of IC detailees and assignees with access to SCI and who were performing joint duty assignments and rotations.[12]

[12] (U) Joint Duty facilitates assignments and details of personnel to national intelligence centers and between elements of the IC.

ICD 709 mandates security reciprocity and precludes additional security, suitability, or fitness reviews for these employees unless:

- the individual's last adjudication was recorded with exceptions;
- information surfaced since the most recent investigation indicating that the individual may no longer satisfy eligibility requirements;
- the most recent investigation is more than seven years old; or
- the individual needs to undergo a polygraph examination to meet the IC element requirements or the existing polygraph is more than seven years old. If a new polygraph examination is needed, the ICD limits the polygraph to a counterintelligence scope only.

(U) Since September 2010, the Special Security Directorate (SSD) within the ODNI Office of the National Counterintelligence Executive/Security has served as the Executive Staff for all Security Executive Agent functions. SSD executes Security Executive Agent responsibilities within the Executive Branch and IC by fostering security uniformity and security clearance reciprocity; performing policy review, coordination, and formulation; promoting uniform application of security policy; enabling the exchange of critical security data; and advising and reporting to the DNI on the implementation of security policies.

IV. (U) OBJECTIVE, SCOPE, AND METHODOLOGY

1. (U) Objective

(U//~~FOUO)~~ This objective was to determine whether there were policies and procedures within the IC that facilitated timely reciprocity of personnel security clearances. Specifically, we assessed the time required to obtain a reciprocal security clearance for three categories of IC personnel:

1. an employee of an IC element who is detailed or assigned to another element of the IC (Detailees and assignees);
2. an employee of an element of the IC seeking permanent employment with another element of the IC (Government transfers); and
3. a contractor working within the IC who is seeking permanent employment with an element of the IC (Contractor conversions).

2. (U) Scope

(U) We assessed the length of time required to obtain a reciprocal security clearance for detailees and assignees, Government transfers, and contractors converting to Government positions who entered on duty with one of six IC elements during FY 2011. We also reviewed policies and processes that may affect the time required to process security clearances for those individuals. We limited our scope to six IC elements:

1) Central Intelligence Agency (CIA),
2) Defense Intelligence Agency (DIA),
3) National Geospatial-Intelligence Agency (NGA),
4) National Reconnaissance Office (NRO),
5) National Security Agency (NSA), and
6) Office of the Director of National Intelligence (ODNI).

(U) We limited our review to individuals who possessed Top Secret/Sensitive Compartmented Information (TS/SCI) clearances, because that is a requirement for all six IC elements. We excluded reciprocity for access to facilities and security clearance reciprocity for contractor personnel who changed employment from one company to another with the same clearance-sponsoring agency, per Intelligence Authorization Act for 2010 requirements.

(U) The security clearance determination, however, is only one piece of the entire hiring process when a detailee or assignee, Government transfer, or contractor converting to a Government position joins another IC element. HR processes and medical evaluations are additional steps in the process. Because HR processes and medical screenings are critical for employment decisions within the IC, we discuss their impact on the hiring process.

3. (U) Scope Limitations

(U) We encountered scope limitations that constrained our ability to assess the extent to which IC elements honor security clearance reciprocity and calculate processing times. Those limitations included unreliable and unavailable data. We discuss those concerns in Appendix C and throughout this report.

(U) **Reliability of Data**. We were unable to rely on all of the computer-processed data provided by IC elements. Although our testing found that some data was sufficiently reliable for the purposes of this report, a significant portion of the data was not reliable and was removed from our analysis. To assess the reliability of data provided by each element, we interviewed officials who provided the data. We also reviewed the data to identify errors in accuracy and completeness. We found unpopulated fields and data entry errors, which we brought to the attention of security, HR, and medical officials who provided the data. We worked with those officials to correct the discrepancies before conducting our analysis. We excluded the records we could not correct. We include limited data on security clearance processing times because of the data limitations (see Appendices B and C for methodology and data limitations).

(U) **Availability of Data.** Data needed to conduct our analysis was not readily available in all instances. According to officials at some IC elements, they did not collect certain data, their databases did not contain all of the requested data, or the effort needed to provide the data would negatively affect their mission. We discuss those challenges in the remainder of this report and in Appendix C.

4. (U) Methodology

(U) To assess the extent to which IC elements honor previously granted reciprocal security clearances and identify requirements for the length of time to process reciprocal security clearances, we reviewed requirements in legislation, Executive Orders, OMB memoranda, and ODNI and element- specific guidance related to security clearance reciprocity.

(U) We interviewed officials from IC element offices of Security, HR, and Medical Services on their policies, procedures, and factors that affect the time it takes for an individual to join their element. We also obtained and analyzed security, medical, and personnel data from each of the elements and tested it for accuracy and completeness. Data included processing start and end dates, status as a detailee or assignee; and entrance-on-duty dates.

(U) We analyzed the data to determine (1) the average length of time to transfer detailees and assignees and to hire Government transfers and contractors converting to Government position; (2) the average time to process security clearances, including reciprocal security clearances; and (3) the average time to complete medical evaluations. We reviewed the data for completeness and accuracy and removed duplicate or incomplete records and records that were not within the scope of the audit.

(U) We analyzed the remaining records for detailees and assignees and Government transfers, and contractor conversions. We then selected a judgmental, non-projectable sample for detailees and assignees; Government transfers; and contractors converting to Government positions. We discussed the samples with officials in HR, security, and medical offices. Our analysis and discussions provided insight into each element's process for honoring security reciprocity and identified factors that affect processing times. (See Appendix B for additional information on the audit methodology.)

5. (U) Compliance with Generally Accepted Government Auditing Standards

(U) We conducted this performance audit from January 2012 through July 2012 in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our objectives.

V. (U) AUDIT RESULTS AND RECOMMENDATIONS

(U) The DNI issued policies to facilitate security clearance reciprocity and the mobility of IC personnel. As the Security Executive Agent, the DNI also is responsible for ensuring the recognition of security clearance reciprocity within the Executive Branch. The Special Security Directorate within the ODNI serves as the Security Executive Agent Executive Staff and executes those responsibilities within the Executive Branch and IC. While SSD recently completed what they consider to be foundational steps necessary to address security clearance reciprocity, SSD had not yet established policies and processes to determine the extent to which the IC elements honor security clearance reciprocity, assessed the amount of time it takes to process requests for security clearance reciprocity, or identified and addressed impediments to granting security clearance reciprocity. Moreover, SSD had not yet established standards for the amount of time it should take to process reciprocal security clearances; established periodic reporting requirements for security clearance reciprocity; or identified the type of data that IC elements should collect to facilitate security clearance reciprocity. Guidance previously issued by the DDNI/PPR, under the authority of the DNI, also did not address those issues.

(U) In addition, IC elements had different interpretations on the applicability of OMB guidance and the use of SF-86s as part of the hiring process and in granting security clearance reciprocity. As a result, the Security Executive Agent did not know whether IC elements were honoring security clearance reciprocity or processing reciprocal security clearances in a timely manner.

(U) The security reciprocity determination is only one piece of the entire hiring process when a detailee or assignee, Government transfer, or contractor who is converting to a Government position joins another IC element. HR Processing, an individual's availability, and medical screenings can lengthen the overall hiring time, even if the individual is eligible for security clearance reciprocity.

1. (U) Security Executive Agent Oversight of Security Clearance Reciprocity

(U) The Security Executive Agent had limited ability to oversee and monitor whether IC elements were processing reciprocal security clearances in a timely manner because the SSD did not issue policies that included reciprocal security clearance timeliness standards or reporting requirements with the type of data elements should collect.

(U) Additionally, the lack of accurate data constrained the ability of the SSD to determine whether IC elements honored security clearance reciprocity or the amount of time it takes to process reciprocal security clearances. As a result, the SSD did not have assurances that IC elements were granting security clearance reciprocity as quickly as possible to facilitate employee mobility while continuing to ensure that security requirements were being satisfied.

(U) **Attempts to Assess Reciprocal Security Clearances.** According to SSD officials, they attempted to obtain security clearance reciprocity data from IC elements in early FY 2012. However, their efforts were unsuccessful because the data submissions were incomplete and could not be compared.

(U) We attempted to obtain and analyze security clearance reciprocity data from the elements to determine the amount of time needed to process reciprocal security clearances. Like SSD, we found that the lack of data constrained our ability to determine if the elements had honored security clearance reciprocity or to assess the amount of time it took the elements to process reciprocal security clearances.

(U) In addition, we identified numerous records at most of the elements that contained missing or incorrect dates and that resulted in total processing times of less than zero days. We also identified records that included transposition errors in social security numbers. The data inaccuracies constrained our ability to assess the extent to which the IC elements honored reciprocal security clearances or the time it took to process them.

(U) The lack of accurate data limited the ability of the Security Executive Agent to oversee and monitor the extent to which the IC Elements honored reciprocal security clearances and the time it took to process them.

(U) **Timeliness Standards**.

- (U) Intelligence Community-Wide Standards. Beginning in 2008, the DDNI/PPR established IC-wide policies that reinforced recognition of reciprocal security clearances within the IC. However, those policies did not establish a common standard for the amount of time it should take to process reciprocal security clearances. Moreover, the SSD has yet to issue Executive Branch-wide policies, to include the IC, that establish common timeliness standards for reciprocal security clearances.

(U) According to SSD officials, their focus and the attention of the IC elements has been on meeting IRTPA timeliness requirements for processing *initial* clearances. IRTPA requires authorized adjudicative agencies to make determinations on at least 90 percent of all applications for a personnel security clearance within an average of 60 days after the date of receipt of the completed application. However, IRTPA does not establish similar timeframes for processing reciprocal security clearances.

(U) SSD officials developed a Security Executive Agent roadmap that identifies milestones for initiatives undertaken by SSD from March 2012 through April 2013. Those initiatives included the development of *National Security and Suitability Investigator and Adjudicator Training Standards* that SSD officials considered to be a foundational step before addressing security clearance reciprocity.

(U) SSD also established a security reciprocity website in March 2012 and planned to implement a national policy on reciprocity in December 2012. SSD officials acknowledged the need to establish guidance for Federal departments and agencies to measure security clearance reciprocity timeliness.

- (U) Intelligence Community Element Standards. Only the ODNI Office of Security established a standard in internal guidance for the length of time to process reciprocal security clearances. In response to work conducted by the ODNI Office of Inspector General[13] and after we initiated this audit, in January 2012 the ODNI Security Office issued internal guidance, *MSD/Security Personnel Clearance Processing for ODNI Personnel*. That guidance established a 7-day timeliness standard for processing security clearances for individuals who hold a current TS/SCI security clearance and a counter-intelligence polygraph and applies to ODNI. According to a senior CIA security official, that guidance was for internal ODNI-use only and did not apply to security clearance reciprocity decisions made by the CIA, which conducts security decisions for ODNI. The ODNI Office of

[13] (U) Office of the Director of National Intelligence Office of Inspector Memorandum, Management Referral Letter, dated 3 October 2011.

Security and the CIA/Office of Security (OS) maintain a service agreement that identifies those security services that CIA/OS performs on behalf of the ODNI. However, the service agreement had not been updated to include the 7-day timeliness standard.

(U) **Periodic Security Clearance Reciprocity Reporting Requirements.** IRTPA and IC policy do not currently include a reporting requirement for security clearance reciprocity or clearly define data that IC elements should collect and report to the SSD to facilitate monitoring and oversight. Also, SSD had not established a requirement that IC elements report security clearance reciprocity data to SSD, nor had SSD required IC elements to collect such data and ensure its accuracy.

(U) According to SSD officials, they have focused on establishing policies and standards that they consider foundational activities for security clearance reciprocity. However, the lack of a periodic reporting requirement for security clearance reciprocity hinders the SSD from gauging program effectiveness and executing oversight responsibilities to ensure reciprocal recognition of access to classified information within the Federal Government. In addition, without clearly defined requirements for the type of data IC elements should collect, the SSD will have limited ability to monitor the effectiveness of the security clearance reciprocity program within the IC.

(U) **Periodic Reporting.** Monitoring programs and processes helps management assess the overall effectiveness and the quality of performance over time. Periodic reporting requirements are one way for management to understand the effectiveness of policies and processes and are an essential component for fulfilling the Security Executive Agent's oversight role.[14] We found that IRTPA and IC-wide policies did not contain a requirement for the IC elements to periodically report to the SSD on the extent to which they honored reciprocal security clearances.[15] SSD officials confirmed that they had not yet established a periodic reporting requirement, as their focus had been on meeting IRTPA timeliness requirements for processing security

[14] (U) United States General Accounting Office, *Standards for Internal Control in the Federal Government*, November 1999 (GAO/AIMD-00-21.3.1).

[15] (U) ICPG 704.4, *Reciprocity of Personnel Security Clearance and Access Determinations* and ICD 709, *Reciprocity of Intelligence Community Employee Mobility.*

clearances, developing a roadmap that identified milestones for initiatives undertaken by SSD, and developing Security and Suitability Investigator and Adjudicator Training Standards. The lack of a periodic reporting requirement for security clearance reciprocity in IC-wide policies hindered the Security Executive Agent from gauging program effectiveness and executing oversight responsibilities.

(U) **Type of Data Collected.** Our review of IRTPA and IC-wide policies found they do not address the type of reciprocity security clearance data that the IC elements should collect. For example, no requirement exists for IC elements to collect data on the number of individuals who were eligible for and received security clearance reciprocity; those who were eligible for security clearance reciprocity but did not receive reciprocity; or the amount of time, on average, to make determinations about reciprocal security clearances. As a result, comparable data was not available from each of the elements. For example:

- (U//~~FOUO~~) CIA OS Integrated Security Tracking and Reporting System (iStars) was not configured to provide security processing data specifically for Government transfers or contractor conversions and, according to CIA HR and OS officials, there was no requirement to do so (see Appendices C and D). According to CIA security officers, a time-intensive manual review of every security action during FY 2011 would be required to provide the requested data.
- (U) DIA does not track data necessary to calculate security clearance processing times for Government transfers and contractor conversions. According to DIA security officials, they reciprocally accept prior clearances upon receipt of favorable notification and pre-employment documentation (such as BI, polygraph, medical screening, and a subject interview). An official also stated that it was DIA policy to automatically process detailees and assignees who were in the IC and who possessed a TS/SCI clearance. Therefore, DIA officials did not collect detailed data for those individuals.
- (U) NGA's database maintained only entry-on-duty dates for detailees and assignees. The database did not contain data on their security clearance processing start or end dates (see Appendix C).

- (U) NRO maintained only entry-on-duty dates for NRO personnel that transferred from another Federal agency. Therefore, the data needed to calculate the total time to transfer those individuals or their security processing times was not available.

- (U) NSA collected data that could be categorized by personnel type, such as detailees and assignees, Government transfers, and contractor conversions. NSA could also identify the number of personnel by category who received reciprocal security clearances (see Appendix C).

(U) According to SSD officials, security clearance reciprocity information was not recorded in Scattered Castles. Identifying the type of data to be collected and measured can help SSD compare actual performance against planned goals and identify unusual trends and areas for corrective action. Requiring comparable data to be available would also facilitate oversight and monitoring. Without clearly defined requirements for the type of data IC elements should collect, the SSD will have limited ability to monitor the effectiveness of the security clearance reciprocity program within the IC.

(U) RECOMMENDATION 1.

1. **(U) The Assistant Director for the Special Security Directorate, in coordination with IC elements, should develop a policy that includes:**

    a. Timeliness standards for reciprocal security clearance processing by IC Elements.

    b. Requirements for the IC elements to report periodically to the Security Executive Agent, or his designee, on security clearance reciprocity.

    c. Metrics and data collection requirements to ensure that data needed to identify the extent to which security clearance reciprocity is honored is available and accurate.

(U//~~FOUO)~~ Management Comments. SSD concurred with this recommendation. SSD is developing Security Executive Agent Directive 600 in which SSD expects to establish metrics for the amount of time to process reciprocal security clearances and to standardize periodic data collection and reporting requirements. SSD anticipates issuing the directive in April 2013 (see Appendix E for the complete SSD comments).

2. (U) Use of Questionnaires for National Security Positions

(U) IC elements had different interpretations concerning the appropriate use of the SF-86 as part of the hiring process, particularly for those individuals who might be eligible for security clearance reciprocity. The lack of an IC-wide policy that clearly describes when applicants who are eligible for security clearance reciprocity should complete an SF-86 has led to different practices among IC elements and may reduce workforce mobility within the IC due to delays that may result from conducting reinvestigations and readjudications.

(U) **OMB Requirements for Using SF-86, *Questionnaire for National Security Positions.*** OMB issued memoranda in 2005 and 2006 that limit the information that Federal agencies may request when determining eligibility for access to classified information when individuals already have current access eligibility with another Government agency and meet certain requirements.[16] Specifically, OMB guidance precludes a gaining agency from requesting that an individual who already has current access eligibility with another Government agency complete a new SF-86, unless a permitted exception to reciprocity exists. Under OMB guidance, Federal agencies are permitted to request that applicants complete a SF-86 when:

- the most recent background investigation is older than 7 years;
- the individual's record has waivers, deviations, or conditions;
- the clearance access on record is an interim clearance; or
- the individual is seeking initial access to a Special Access Program.

(U//~~FOUO)~~ **IC elements' Use of SF-86.** IC elements had different interpretations on the use of the SF-86 as part of the hiring process. For example, the CIA and ODNI required all individuals seeking permanent employment with CIA or ODNI to complete an SF-86 as part of the hiring process, even if the individual might qualify for security clearance reciprocity.

[16] (U) OMB. *Reciprocal Recognition of Existing Personnel Security Clearances, Checklist of Permitted Exception,* 12 December 2005, revised 17 July 2006.

(U) According to CIA officials, the updated SF-86 helped to ascertain whether any new developments had taken place since the last adjudication that might call their eligibility for access to classified information into question. Those developments include any changes to:

- loyalty to the United States;
- family, citizenship, education, employment, residence history, and military service;
- financial situation;
- psychological conditions;
- use of alcohol or drugs;
- involvement in criminal activity;
- foreign travel; and
- association with foreign nationals.[17]

(U//~~FOUO~~) CIA officials stated that without obtaining an updated SF-86, they might not otherwise be aware of concerns that occurred between periodic reinvestigations. A senior CIA security officer asserted that while reciprocity streamlines the security clearance process, any additional processing time incurred through submission of an updated SF-86 was negligible compared to the national security implications if updated information that might disqualify an individual from employment was missed in the interest of enhancing workforce mobility. A DIA official concurred with the CIA practice stating that the SF-86 provided information that might warrant a reinvestigation of an individual. However, according to SSD officials and ODNI General Counsel, the SF-86 should not be sent to applicants who are eligible for reciprocity.

(U) Other IC elements, such as NGA, do not require that all new applicants complete or update an SF-86. NGA first verifies whether an applicant is eligible for security clearance reciprocity and requires only those individuals who are ineligible for security clearance reciprocity to update an SF-86.

[17] (U) Intelligence Community Policy Guidance 704.1, *Personnel Security Investigative Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information*, 2 October 2008.

(U) **IC-Wide Policy for the Use of Standard Forms-86.** The lack of an IC-wide policy that clearly describes when an SF-86 should be completed or updated by applicants who are eligible for security clearance reciprocity has led to different practices among the IC elements. Requiring applicants who may be eligible for security clearance reciprocity to update an SF-86 as part of the hiring process can mitigate potential risks to national security that may have developed since the applicant's last investigation. However, using changes in security sponsorship as an opportunity to learn about new developments that might affect access to classified information can lengthen the processing time for an applicant and reduce workforce mobility, which contradicts a goal of security clearance reciprocity.

(U) RECOMMENDATION 2.

2. (U) The Assistant Director for the Special Security Directorate should:

a. Develop an IC-wide policy that clearly explains the requirements or prohibition of use of the SF-86 when applicants are eligible for security clearance reciprocity.

b. Implement internal controls to monitor IC element compliance with the policy that explains the use of the SF-86.

(U//~~FOUO)~~ Management Comments. SSD concurred with the recommendation. SSD plans to include specific guidance in Security Executive Agent Directive 600 to address the circumstances when an agency can request completion of an SF-86 in connection with the processing of an existing security clearance that may be eligible for reciprocity. Beginning in February 2013, SSD also plans to initiate assessments of Executive Branch agency performance in applying security clearance reciprocity as part of the security clearance process (see Appendix E for the complete comments from SSD).

3. (U) Other Matters of Interest

(U) The Intelligence Authorization Act for FY 2010 does not direct us to assess factors other than the time to process reciprocal security clearances for detailees and assignees, Government transfers, and contractor conversions. However, the processing of reciprocal security clearances alone does not present a complete picture of the time it takes to reassign or hire personnel into an IC element. Other factors, such as (1) internal processes for reassigning and transferring personnel; (2) determinations regarding an individual's eligibility for security clearance reciprocity; (3) human resources (HR) hiring processes; and (4) medical screening. affect the time it takes for an individual to transfer or join an IC element. Because those factors were outside the scope of our audit, we did not perform a comprehensive evaluation of all related policies, processes, and their impact on processing times. We are providing those factors for informational purposes only and do not make any recommendations to address them.

(U) **IC element Processes to Reassign and Hire Personnel.** IC elements did not have the same suitability requirements, which could contribute to delays in reassigning and hiring personnel (see Table 1.) For example, CIA and NSA use full scope polygraphs to evaluate if individuals are suitable for employment.[18] Other IC elements use only counterintelligence (CI) scope polygraphs.[19] In addition, most IC elements require medical screening.

[18] (U) A full scope polygraph (also known as expanded scope polygraph) asks the candidate questions concerning counterintelligence issues as well as suitability concerns such as use of illegal drugs, involvement in serious criminal activity, and falsification of security forms.

[19] (U) A counterintelligence polygraph asks the candidate questions limited to those necessary to determine whether the examinee ever had any involvement with or knowledge of espionage/sabotage against the United States, unauthorized Foreign National contacts, unauthorized disclosure of classified material, terrorist activities or deliberate damage to or malicious misuse of a U.S. Government information and/or defense systems.

(U//~~FOUO) T~~able 1: Reciprocity and Other Employment Requirements for Government Transfers and Contractor Conversions by IC Element

IC Element[1]	Reciprocity Requirements		Other Employment Requirements		
	TS/SCI	BI	Polygraph		Medical Screening
			Full scope	CI	
CIA	✓	✓	✓		✓
DIA	✓	✓		✓	✓
NGA	✓	✓		✓	✓[2]
NSA	✓	✓	✓		✓
ODNI	✓	✓		✓	✓

(U) Source: IC IG analysis.
(U) Notes:
(U) [1]NRO information is omitted from the table because the NRO is staffed by detailees and assignees and does not have government transfers or contractor conversions.
(U) [2]NGA medical evaluations are limited to eye examinations for Imagery Analysts and physicals for certain security positions. Other NGA positions do not require medical examinations.

(U) **Ineligibility for Security Clearance Reciprocity.** Not all individuals are eligible for security clearance reciprocity, even when they have a BI, hold a TS/SCI clearance, and work within the IC. Our analysis of data provided by the IC elements and discussions with security officials found that some individuals were not eligible for reciprocal security clearances for the following reasons:

- their BIs were out of scope;
- they did not meet polygraph requirements for the position;
- they had deviations, waivers, or conditions to their BIs;
- they had breaks in service; or
- there were counterintelligence concerns.

(U) Individuals who fell into those categories typically required lengthier processing times because those issues had to be addressed and resolved.

(U) **Human Resource Hiring Processes and Availability of Individuals.** We identified factors that influenced—and in most cases increased—the amount of time it took to reassign or hire an individual into an IC element. Analysis of our data sample and discussions with HR officials identified applicant preferences for delayed start dates, military deployments, applicant cancellations of polygraph sessions, and delays in submitting paperwork as factors out that lengthened the hiring processing time and were outside the control of the IC element. Different hiring practices at each IC element was another factor. For example, NGA made conditional offers of employment that were not always associated with an available billet. The applicant was processed and may have met all hiring requirements, but still had to wait for a billet to become available.

(U//~~FOUO~~) **Medical Screenings.** Medical evaluations determine if an individual meets physical and psychological standards for employment or assignment within the IC. Although medical requirements may differ, they frequently include mental health evaluations and physical screenings such as hearing and vision exams and lab work. Medical evaluations can be lengthened by:

- the requirement for applicants to provide additional information from personal physicians for a medical condition; and
- reviews by IC Element medical personnel of potentially disqualifying medical conditions.

(U) According to CIA HR and medical officials, a memorandum of understanding (MOU) with other IC elements to reciprocally accept prior medical examinations would shorten medical screening processing times. CIA Office of Medical Services officials stated that CIA had established medical reciprocity MOUs with IC elements that had medical infrastructure and medical requirements that were similar to the CIA.

VI. (U) Conclusion

(U) Security clearance reciprocity has the potential to increase the mobility of Federal workers across the IC to support mission critical needs and to conserve resources. However, the Security Executive Agent lacks visibility and assurance that IC elements are honoring reciprocity and processing eligible individuals as quickly as possible. Although the focus on delays in hiring or transferring employees is often placed on the security clearance determination process, it is just one part of the process of vetting individuals for hire by an IC element. Other factors, such internal processes for reassigning and transferring personnel; determinations regarding an individual's eligibility for security clearance reciprocity; HR hiring processes; and medical screening also affect the length of the hiring process.

(U) Appendix A: Abbreviations

(U) BI	Background Investigation
(U) CI	Counter Intelligence
(U) CIA	Central Intelligence Agency
(U) COE	Conditional Offer of Employment
(U) DIA	Defense Intelligence Agency
(U) DDNI/PPR	Deputy DNI/Policy, Plans, and Requirements
(U) DNI	Director of National Intelligence
(U) EOD	Entered on Duty
(U) EO	Executive Order
(U) FY	Fiscal Year
(U) HR	Human Resources
(U) IC	Intelligence Community
(U) ICD	Intelligence Community Directive
(U) IC IG	Inspector General for the Intelligence Community
(U) ICPG	Intelligence Community Policy Guidance
(U) IRTPA	Intelligence Reform and Terrorism Prevention Act
(U) iSTARS	Integrated Security Tracking and Reporting Systems
(U) MOU	Memorandum of Understanding
(U) MSD	Mission Support Division
(U) NGA	National Geospatial Intelligence Agency
(U) NRO	National Reconnaissance Office
(U) NSA	National Security Agency
(U) ODNI	Office of the Director of National Intelligence
(U) OMB	Office of Management and Budget
(U) OMS	Office of Medical Services
(U) OS	Office of Security
(U) PSD	Personnel Security Division
(U) SF-86	Standard Form-86
(U) SSD	Special Security Division
(U) TS/SCI	Top Secret/Sensitive Compartmented Information

(U) Appendix B: Detailed Methodology

(U) This Appendix contains detailed information on how we calculated processing times and the sampling methodology.

1. (U) Calculation of Processing Times

(U) To determine the average amount of time to process detailees and assignees at each IC element, we evaluated the number of days from the date when the hiring process was initiated to the date when the applicant entered–on-duty (EOD). For Government transfers and contractor conversions, we calculated the number of days from the receipt of the signed conditional offer of employment (COE) or equivalent by the HR department to the EOD date. We refer to those calculated lengths of time as the total processing time.

(U) To determine security processing times for detailees and assignees, Government transfers, and contractor conversions to complete security processing, we calculated the number of days from the date HR requested a security review of an individual to the date when Security informed HR that the security review was complete. Due to data limitations discussed in the remainder of this Appendix, we were not able to determine security processing times for all categories of personnel.

(U) To determine medical processing times for detailees and assignees, Government transfers, and contractor conversions, we calculated the number of days from the date HR requested a medical evaluation of an individual to the date when medical officials informed HR that the medical evaluation was complete. We limited our analysis of medical processing times to those IC elements and positions that had a medical requirement.

2. (U) Data Samples

(U) At each IC element, we selected a judgmental, non-projectable sample for each category of personnel. We selected the samples using the mean and standard deviations for the total processing time.[20] The standard deviations allowed us to identify individuals who experienced total processing times that were significantly longer than the average processing time for the respective IC element and personnel category. We refer to those records as "outliers." For each sample, when selecting records for additional analysis, we used the benchmark of greater than two standard deviations.

(U//~~FOUO)~~ Because of the large number of records from the CIA, we used three standard deviations as our benchmark for selecting additional records from that IC element. For NRO, we used the outliers in the average security processing time because NRO did not have a centralized database that contained EOD information for individuals who required additional security processing. We also judgmentally selected records that were below or near the average total processing time for inclusion in each sample. The sample size varied by the population at each IC element who were hired during FY 2011 (see Table 2).

[20] (U) Standard deviation is a measure of variability and shows how much variation exists from the average. In a normal distribution, nearly all values lie within three standard deviations of the mean. According to the empirical rule, about 68 percent of the values lie within one standard deviation of the mean; about 95 percent of the values lie within two standard deviations of the mean; and about 99 percent of the values lie within three standard deviations of the mean.

(U//~~FOUO~~) Table 2: IC Element Population and Sample Sizes

IC Element	Population			Sample Size		
	Detailees/ Assignees	Government Transfers	Contractors Conversions	Detailees/ Assignees	Government Transfers	Contractors Conversions
CIA	417	---[1]		15	---[1]	
DIA	30	734		---[2]	25	
NGA	415	265		---[2]	16	
NRO	116[3]	Not Applicable[5]		9	Not Applicable[5]	
	733[4]	Not Applicable[5]		5	Not Applicable[5]	
NSA[6]	15	4	217	5	4	17
ODNI	255	77		19	12	

(U) Source: IC IG analysis of IC element data.
Notes:
(U) [1] Given the manner in which the CIA's Office of Security records and tracks personnel data, the CIA could not generate a list that separated Government transfers and contractor conversions from all new hires. Therefore, we judgmentally selected 15 individuals from a list provided by CIA HR and OMS. However, according to Security and HR officials, the selected sample did not include individuals who were Government transfers or contractor conversions. Therefore, the sample was not within the scope of this audit.
(U) [2] DIA and NGA did not maintain data for detailees and assignees.
(U) [3] NRO reciprocally accepted the background investigations for these detailees and assignees. However, before EOD, these individuals required additional security processing to meet NRO's security requirements.
(U) [4] NRO officials stated that these individuals received security clearance reciprocity. However, NRO collected only EOD dates.
(U) [5] The NRO workforce is comprised of detailees and assignees from other agencies.
(U) [6] NSA only provided data for personnel who received reciprocal security clearances. NSA considers an individual as eligible for security clearance reciprocity when an individual possesses a TS/SCI clearance, a current background investigation, and a full scope polygraph.

(U) We discussed the samples with IC element officials from security, HR, and medical offices. Those discussions tested the validity of the sample data; provided insight into each element's process for honoring security reciprocity; and other factors that affected processing times. Our discussions also provided insight into determinations of eligibility for reciprocal security clearances.

(U) Appendix C: Data Limitations at Each IC Element

(U) We encountered data limitations that constrained our ability to assess the extent to which each IC element honored security clearance reciprocity and limited our ability to calculate reciprocal security clearance and medical evaluation processing times. We reviewed data obtained from IC elements for completeness and accuracy and removed duplicate, incomplete, and out of scope records. Table 3 summarizes the number of records that we removed.

(U//FOUO) Table 3: Records Provided by IC Elements and Removed

IC Element	Total Records Provided	Records Removed	Net Records
CIA	2,561	2,144[1]	417
DIA	1,000	266	734
NGA	695	430	265
NRO	849	733[2]	116
NSA	240	4	236
ODNI	443	111	332

(U) Source: IC IG analysis of IC element data.

(U) Notes:

(U) [1]We removed CIA records that either contained data errors or for which we could not develop a complete record that consisted of HR, security, and medical information for an individual due to the way that component databases and systems collected and maintained data to meet their business requirements. The 2,144 records that we excluded from our analysis included 1,113 records, which we reviewed to obtain an understanding of factors that affected security and overall processing times. However, we did not calculate the actual time to process those individuals or the amount of time CIA security took to make security clearance determinations because CIA security systems did not record and track data in a way that allowed them to easily identify and segregate Government transfers and contractor conversions from all new hires.

(U) [2]We removed the majority of records for NRO personnel that transferred from another Federal agency. NRO officials stated that although those individuals received reciprocity, NRO maintained only EOD dates. Therefore, we were not able to calculate the total time to transfer those individuals or their security processing times.

(U) The following sections present information on the data limitations we encountered by IC element and the categories of individuals in the scope of this audit.

1. (U) Central Intelligence Agency

(U//~~FOUO~~) **Government Transfers and Contractor Conversions.** CIA HR provided a list from its E-Recruiting database of all individuals who entered on duty with the CIA in FY 2011. CIA Office of Medical Services (OMS) used the list to compile medical processing data from the Medical Information

Comprehensive System (MEDICS) database. According to CIA officials, E-Recruiting and MEDICS were not configured to separate Government transfers and contractors who converted to Government positions from other new hires. CIA Office of Security (OS) officials also could not provide data specifically for Government transfers and contractor conversions because of the way their database is set-up, and stated that an intensive manual review of each individual record would be required to provide data limited to Government transfers and contractor conversions because data extracted from the Integrated Security Tracking and Reporting Systems (iStars) database would include individuals that were outside of our scope. OS officials also explained that iStars captured security actions by fiscal year, not by EOD date. Given those constraints, we were not able to determine the average total processing time, security-processing time, or medical processing time for Government transfers and contractor conversions.

(U//~~FOUO)~~ **Detailees and Assignees.** CIA HR identified detailees and assignees who EOD at the CIA in FY 2011. CIA OS and OMS used that information to provide corresponding medical information to calculate processing times for detailees and assignees. CIA OS provided dates associated with security actions for the identified detailees and assignees in FY 2011. CIA OIG merged the HR, OMS, and OS data into one list consisting of 1,432 records. Because CIA conducts security reviews and medical evaluations for ODNI detailees and assignees, that list included 428 ODNI detailees and assignees. We removed those ODNI records, leaving 1,004 records in the CIA detailee and assignee population. Next, we removed 587 records that contained data errors or that did not contain data from both OS and HR due to the way their systems were set up. The resulting population consisted of 417 records that contained information from HR, OMS, and OS.

2. (U) Defense Intelligence Agency

(U//~~FOUO)~~ **Government Transfers and Contractor Conversions**. The DIA Counterintelligence and Security Activity Division provided a list of 970 records for civilian applicants who entered on duty during FY 2011 and were included in the DIA HR database, EzHR. According to DIA officials, the list did not include military applicants or individuals whose records contained missing or inaccurate data. We eliminated 236 records with negative total processing times or with missing data that precluded us from determining the overall processing times.

(U) DIA Counterintelligence and Security Activity manually tracked security-processing data in its Personnel Security System (PS3). However, PS3 did not have a report capability, which prevented us from using the data for our analysis. According to DIA officials, DIA is digitizing security records to facilitate electronic processing and tracking reciprocal security clearances. DIA is also developing a system that — when ready in 2015 — will process all security actionsto include final security clearance determinations and reciprocal security clearance status.

(U//~~FOUO)~~ **Detailees and Assignees.** The DIA Human Capital Division identified 30 individuals who were detailed or assigned to DIA in FY 2011. DIA collected limited data on detailees and assignees, such as their home agency, pay band, title, and assignment start and end dates. An official from DIA's Joint Duty Assignment Office stated that their office did not include detailees and assignees in the EzHR database, nor did they track medical, security, or HR information for those individuals. As a result, the data we needed to determine the total hiring processing times or security-processing times was unavailable.

3. (U) National Geospatial-Intelligence Agency

(U//~~FOUO)~~ **Government Transfers and Contractor Conversions.** The NGA Human Development Directorate and the Security and Installation Directorate provided a list of 280 applicants from its PeopleSoft database who NGA identified as having received security clearance reciprocity during FY 2011. We eliminated 15 records from our analysis because the processing time for each record was negative, and NGA officials did not provide corrected data. According to NGA officials, those 15 individuals changed positions within the NGA. In those cases, the NGA database included the new position information and dates, but retained the original security data, resulting in negative and inaccurate processing times.

(U//~~FOUO)~~ **Detailees and Assignees.** NGA provided information on IC employees that were assigned long-term to NGA and who performed NGA functions, which it calls "Affiliates." NGA refers to employees of other Government agencies who are temporarily assigned to NGA as

"Other Government Agency Personnel." For purposes of this report, we refer to those employees as detailees and assignees when discussing NGA. NGA identified 415 detailees and assignees with EOD dates at NGA in FY 2011. For those individuals, NGA only provided the date the individual reported for duty. An NGA HR officer stated that NGA had little, if any, hiring data for those individuals in its PeopleSoft database. As a result, we were not able to determine the total and security processing times.

4. (U) National Reconnaissance Office

(U//~~FOUO~~) **Government Transfers and Contractor Conversions**. NRO is a joint civilian agency staffed solely with detailees and assignees from other IC elements, Department of Defense civilians, and military personnel. As such, NRO had no Government transfers or contractor conversions.

(U//~~FOUO~~) **Detailees and Assignees.** The NRO Personnel Security Division (PSD) and the Office of Strategic Human Capital identified individuals detailed or assigned to NRO during FY 2011. PSD identified 116 individuals with TS/SCI clearances in its security database, the Access Polygraph Investigative Collection System. Those individuals required additional suitability security processing to meet NRO's security requirements before entering on duty. However, NRO reciprocally accepted their background investigations. Each NRO component maintained hiring information, such as the date the hiring process was initiated and the EOD date. NRO did not maintain HR information in a centralized database. Because of the impracticality of receiving that data from each individual component, we used data obtained from the PSD security database to select our sample and perform our analysis.

(U//~~FOUO)~~ The Office of Strategic Human Capital identified 733 individuals in its SAP HR Information System who were detailees or assignees from another Federal agency during FY 2011. Those individuals held security clearances that met or exceeded the NRO security clearance requirement of TS/SCI and subject to a CI polygraph. Therefore, those individuals did not require additional security processing. PSD officials stated that they verified that the background investigation and polygraph were in scope for those individuals. NRO was not able to provide the data we needed to determine the total processing times or security processing times for those individuals because the NRO did not track that information. We selected five records from the PSD-provided data for discussion with NRO officials to gain an understanding of the NRO processes for honoring security clearance reciprocity.

5. (U) National Security Agency

(U//~~FOUO~~) **Government Transfers and Contractor Conversions**. The NSA Office of Personnel Security, HR, and the Office of Health, Environmental, and Safety Services identified 4 Government transfers and 217 contractors that converted to Government positions and received security clearance reciprocity during FY 2011, according to its PeopleSoft database. NSA considers an individual who possesses a TS/SCI clearance, a current BI, and a full scope polygraph to be eligible for security clearance reciprocity. NSA did not provide data for individuals who had TS/SCI clearances but were ineligible for security clearance reciprocity due to out-of-scope background investigations, BIs with exceptions, or who required updated or full-scope polygraphs.

(U) When discussing our sample for contractor conversions with NSA, we determined that some of the data provided resulted in abnormally long processing times because multiple conditional job offers were made to the individual. NSA provided corrected data and we selected a new sample and discussed those records with officials to identify factors that affected processing times and eligibility for security clearance reciprocity.

(U//~~FOUO~~) **Detailees and Assignees.** The NSA Office of Personnel Security identified 15 detailees and assignees EOD FY 2011. However, similar to the Government transfers and contractor conversions, NSA only provided data for individuals they determined were eligible for security clearance reciprocity. We selected five records for discussion with NSA officials to gain insight into factors that affected processing times.

6. (U) Office of the Director of National Intelligence

(U//~~FOUO~~) **Government Transfers and Contractor Conversions.** ODNI/ Mission Support Division (MSD)/HR identified 77 Government transfers and contractor conversions who entered on duty with the ODNI during FY 2011. ODNI/MSD/HR compiled that information from manual reviews of emails from security and medical officials, the ODNI Recruiting and Staffing Database, and the HR Action Tracker Database. We provided that list to CIA OS and CIA OMS because they conduct security processing and medical evaluations on behalf of ODNI. CIA OS provided data for all but 30 individuals who they determined were not eligible for security clearance reciprocity. CIA OMS officials provided data for individuals who were in its MEDICS database and also on the ODNI/ MSD/HR list. OMS explained that those individuals entered on duty with ODNI before OMS began providing medical evaluations of ODNI candidates and, therefore, were not required to complete a medical evaluation.

(U//~~FOUO~~) **Detailees and Assignees.** ODNI/MSD/HR identified 255 detailees and assignees who entered on duty with the ODNI during FY 2011. CIA OS provided the data to permit us to calculate the security processing times for those detailees and assignees. ODNI does not require medical processing for detailees and assignees; therefore, we did not request data from CIA OMS for those individuals.

(U) Appendix D: Data Analysis Results

(U) We attempted to obtain and analyze security clearance reciprocity data from IC elements to determine the amount of time needed to process reciprocal security clearances. Given the constraints resulting from variances in the type, availability, and accuracy of data collected by those elements, we conducted a limited analysis of reciprocal security clearance data. The results of our analysis are presented in this appendix.

1. (U) Detailees and Assignees

(U//~~FOUO~~) We analyzed data provided by CIA, NRO, and ODNI to determine the average number of days and range of days to process security clearances for detailees and assignees, as shown in Table 4. Not all of those individuals were necessarily eligible for security clearance reciprocity.

(U//~~FOUO~~) Table 4: Average Number of Days for IC elements to Make Security Clearances Determinations for Detailees and Assignees During FY 2011.

IC Element	Average (in days)[1]	Range (in days)[1,2]	Population
CIA	12	0 to 269	417
NRO	40	1 to 211	116
ODNI	8	0 to 277	255

(U) Source: IC IG analysis of data provided by CIA, NRO, and ODNI.
(U) Notes:
(U) [1] Numbers are rounded to nearest whole number.
(U) [2] "0" indicates same day processing.

(U) DIA and NGA did not collect all of the data that we required to calculate security-processing times for detailees and assignees. According to a security official, it is DIA policy to automatically process detailees and assignees who are in the IC and who possess a TS/SCI clearance. According to NGA, it collects little hiring data for detailees and assignees.

(U//~~FOUO~~) NSA provided data that showed it processed reciprocal security clearances in an average of 1 day for 15 detailees and assignees who it determined were eligible for reciprocal security clearances and who entered on duty during FY 2011. NSA only provided data for individuals they determined were eligible for security clearance reciprocity; therefore, we could not determine the extent that NSA honored reciprocal security clearances for all detailees and assignees.

2. (U) Government Transfers and Contractor Conversions

(U) NGA, NSA, and ODNI provided data to calculate the number of days, on average, to process reciprocal security clearances for Government transfers and contractor conversions, shown in Table 5.

(U//~~FOUO)~~ Table 5: Average Number of Days for IC elements to Make Reciprocal Security Clearances Determinations for Government Transfers and Contractor Conversions During FY 2011.

IC Element	Average (in days)[1]	Range (in days)[1,2]	Population
NGA	9	0 to 452	265
NSA			
Government transfer	[redacted]	[redacted]	[redacted]
Contractor conversion	[redacted]	[redacted]	[redacted]
ODNI	62	0 to 554	77

(U) Source: IC IG Analysis of data provided by NGA, NSA and ODNI.

(U) Notes:

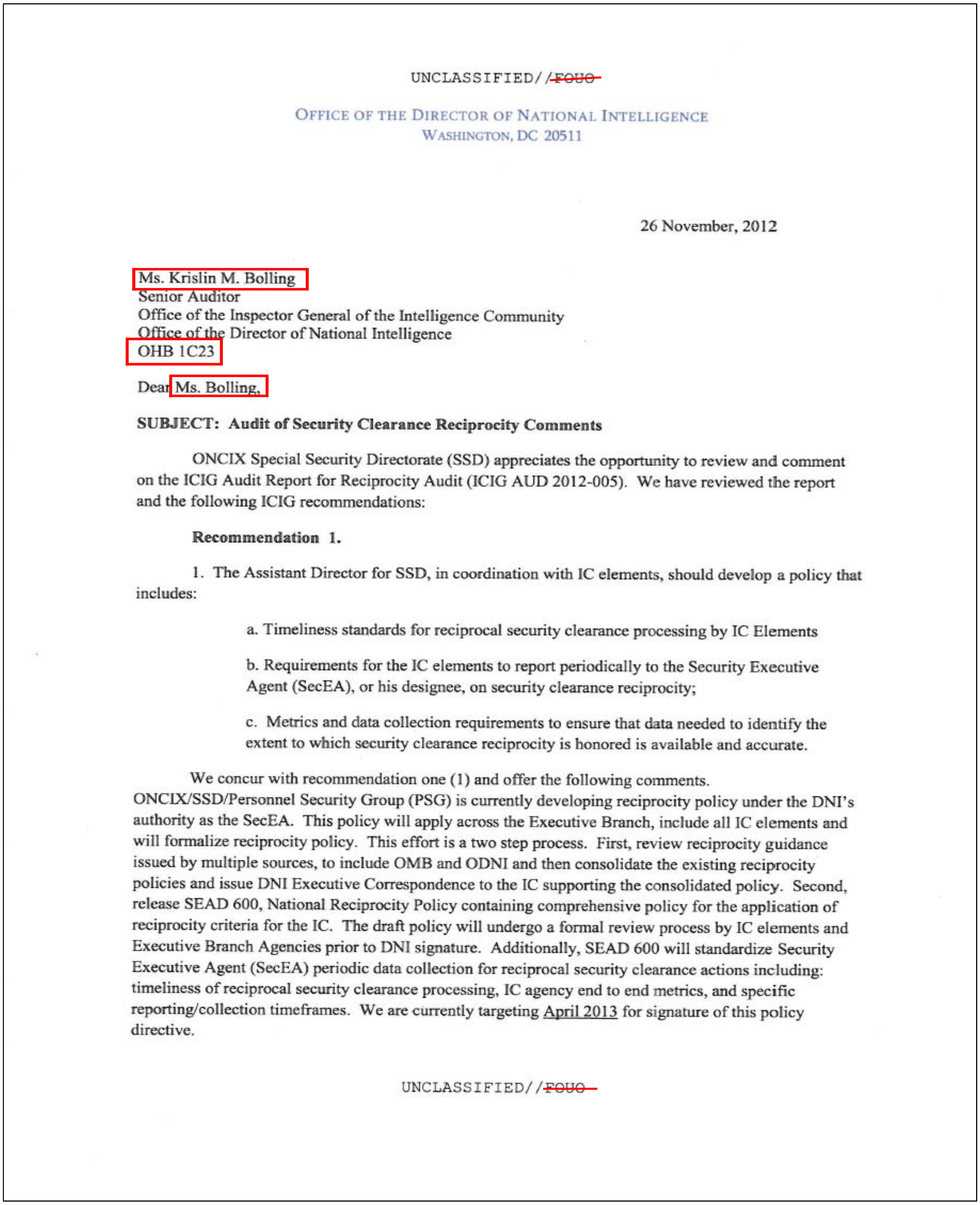
(U) [1]Average number of days and range are rounded to the nearest whole number.

(U) [2]"0" indicates same-day processing.

(U//~~FOUO~~) We were unable to include information on DIA, CIA, and NRO in Table 5 for the following reasons:

- (U) DIA does not track data we needed to calculate security clearance processing times for Government transfers and contractor conversions. According to DIA security officials, they reciprocally accept prior clearances upon receipt of favorable notification and pre-employment documentation (e.g., BI, polygraph, medical screening, and a subject interview).
- (U) As previously discussed, the CIA OS could not provide data specifically for Government transfers or contractor conversions because their security database is not configured to identify those types of individuals and there was no business requirement to do so. According to CIA security officers, a time-intensive manual review of every security action during FY 2011 was required to provide the requested data.
- (U) NRO is a joint civilian agency staffed by detailees and assignees from other IC elements, Department of Defense civilians, and military personnel. As such, NRO does not process Government transfers or contractor conversions.

(U) Appendix E: Management Comments



UNCLASSIFIED//~~FOUO~~

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

26 November, 2012

Ms. Krislin M. Bolling
Senior Auditor
Office of the Inspector General of the Intelligence Community
Office of the Director of National Intelligence
OHB 1C23

Dear Ms. Bolling,

SUBJECT: Audit of Security Clearance Reciprocity Comments

ONCIX Special Security Directorate (SSD) appreciates the opportunity to review and comment on the ICIG Audit Report for Reciprocity Audit (ICIG AUD 2012-005). We have reviewed the report and the following ICIG recommendations:

Recommendation 1.

1. The Assistant Director for SSD, in coordination with IC elements, should develop a policy that includes:

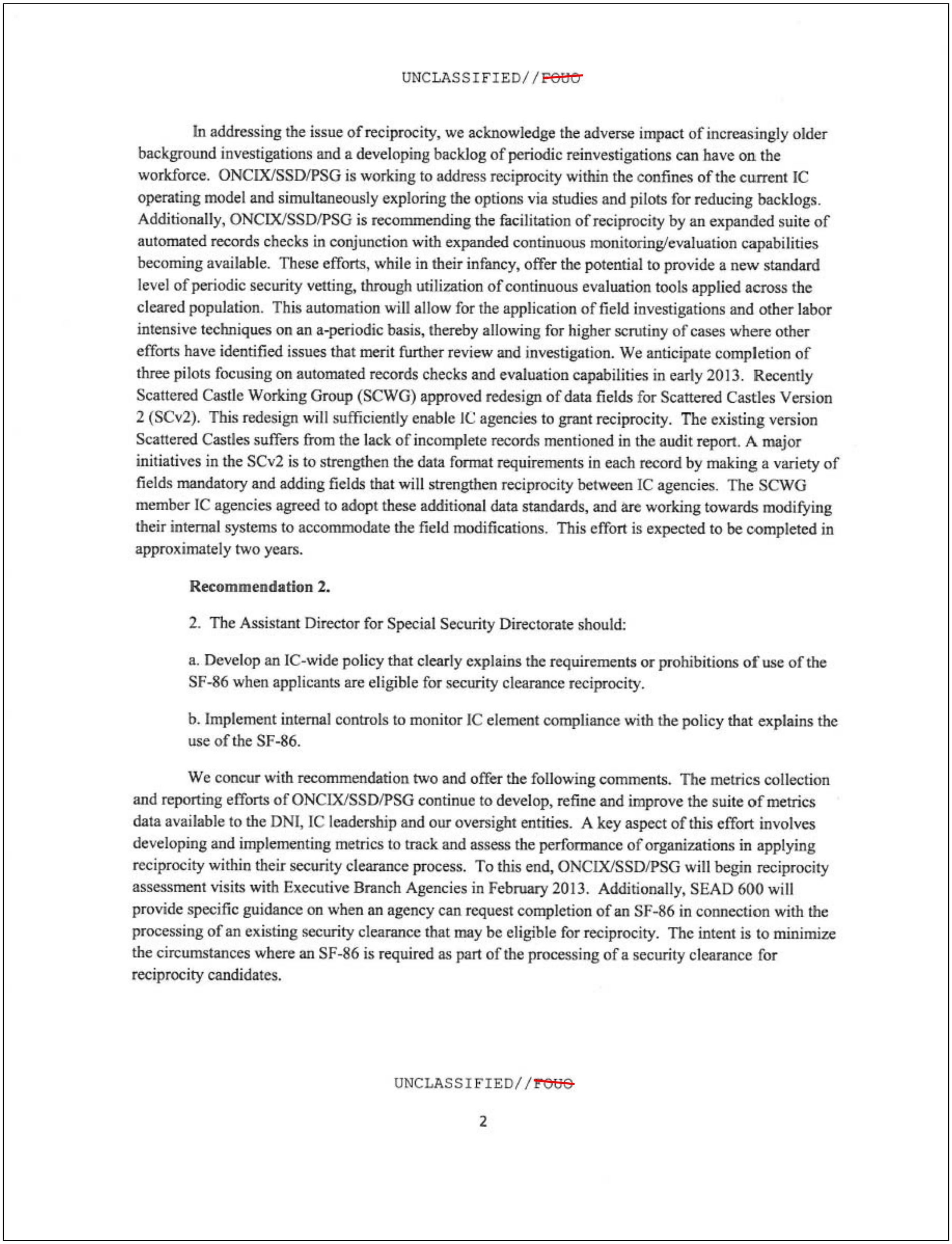
a. Timeliness standards for reciprocal security clearance processing by IC Elements

b. Requirements for the IC elements to report periodically to the Security Executive Agent (SecEA), or his designee, on security clearance reciprocity;

c. Metrics and data collection requirements to ensure that data needed to identify the extent to which security clearance reciprocity is honored is available and accurate.

We concur with recommendation one (1) and offer the following comments. ONCIX/SSD/Personnel Security Group (PSG) is currently developing reciprocity policy under the DNI's authority as the SecEA. This policy will apply across the Executive Branch, include all IC elements and will formalize reciprocity policy. This effort is a two step process. First, review reciprocity guidance issued by multiple sources, to include OMB and ODNI and then consolidate the existing reciprocity policies and issue DNI Executive Correspondence to the IC supporting the consolidated policy. Second, release SEAD 600, National Reciprocity Policy containing comprehensive policy for the application of reciprocity criteria for the IC. The draft policy will undergo a formal review process by IC elements and Executive Branch Agencies prior to DNI signature. Additionally, SEAD 600 will standardize Security Executive Agent (SecEA) periodic data collection for reciprocal security clearance actions including: timeliness of reciprocal security clearance processing, IC agency end to end metrics, and specific reporting/collection timeframes. We are currently targeting April 2013 for signature of this policy directive.

UNCLASSIFIED//~~FOUO~~



In addressing the issue of reciprocity, we acknowledge the adverse impact of increasingly older background investigations and a developing backlog of periodic reinvestigations can have on the workforce. ONCIX/SSD/PSG is working to address reciprocity within the confines of the current IC operating model and simultaneously exploring the options via studies and pilots for reducing backlogs. Additionally, ONCIX/SSD/PSG is recommending the facilitation of reciprocity by an expanded suite of automated records checks in conjunction with expanded continuous monitoring/evaluation capabilities becoming available. These efforts, while in their infancy, offer the potential to provide a new standard level of periodic security vetting, through utilization of continuous evaluation tools applied across the cleared population. This automation will allow for the application of field investigations and other labor intensive techniques on an a-periodic basis, thereby allowing for higher scrutiny of cases where other efforts have identified issues that merit further review and investigation. We anticipate completion of three pilots focusing on automated records checks and evaluation capabilities in early 2013. Recently Scattered Castle Working Group (SCWG) approved redesign of data fields for Scattered Castles Version 2 (SCv2). This redesign will sufficiently enable IC agencies to grant reciprocity. The existing version Scattered Castles suffers from the lack of incomplete records mentioned in the audit report. A major initiatives in the SCv2 is to strengthen the data format requirements in each record by making a variety of fields mandatory and adding fields that will strengthen reciprocity between IC agencies. The SCWG member IC agencies agreed to adopt these additional data standards, and are working towards modifying their internal systems to accommodate the field modifications. This effort is expected to be completed in approximately two years.

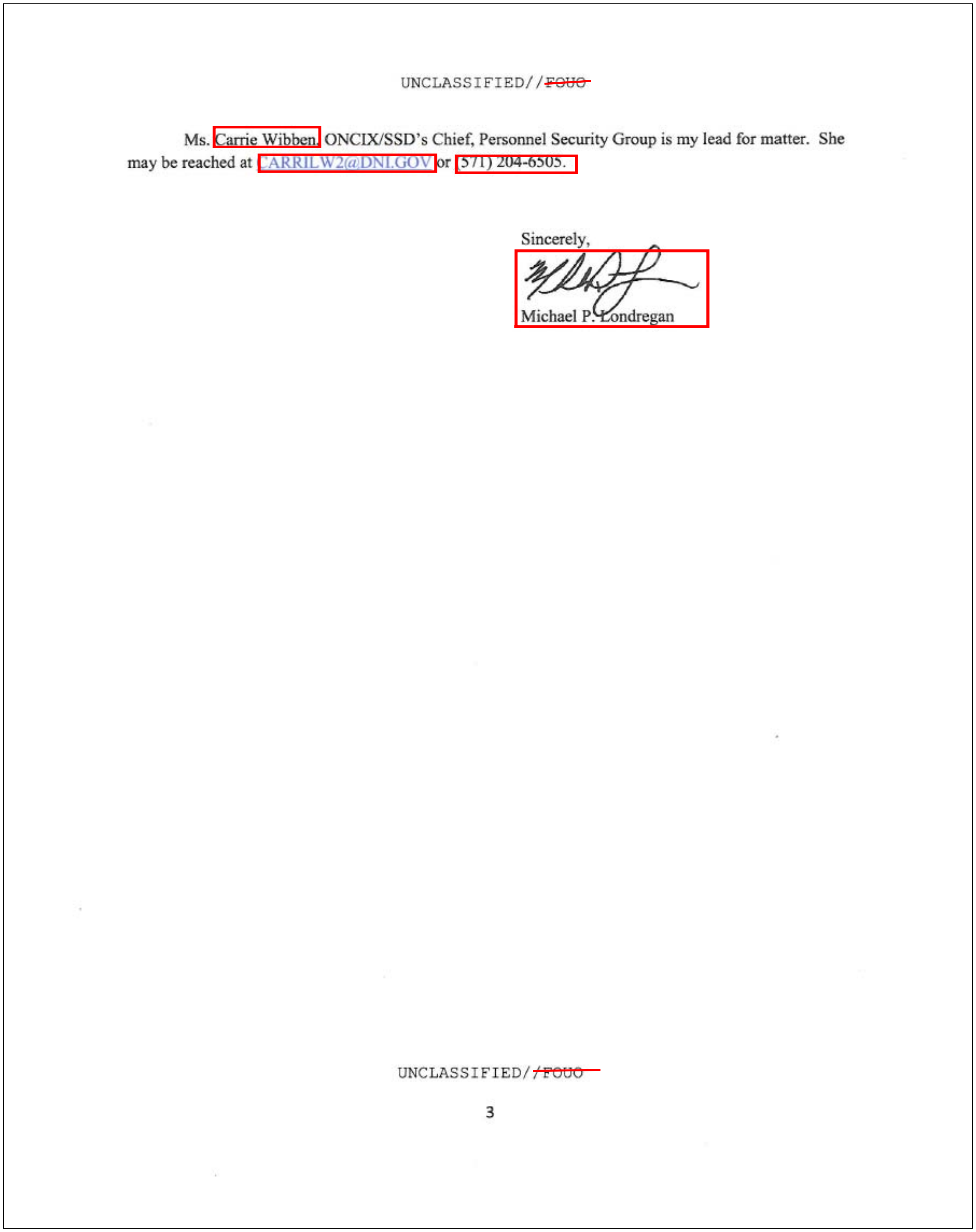
Recommendation 2.

2. The Assistant Director for Special Security Directorate should:

a. Develop an IC-wide policy that clearly explains the requirements or prohibitions of use of the SF-86 when applicants are eligible for security clearance reciprocity.

b. Implement internal controls to monitor IC element compliance with the policy that explains the use of the SF-86.

We concur with recommendation two and offer the following comments. The metrics collection and reporting efforts of ONCIX/SSD/PSG continue to develop, refine and improve the suite of metrics data available to the DNI, IC leadership and our oversight entities. A key aspect of this effort involves developing and implementing metrics to track and assess the performance of organizations in applying reciprocity within their security clearance process. To this end, ONCIX/SSD/PSG will begin reciprocity assessment visits with Executive Branch Agencies in February 2013. Additionally, SEAD 600 will provide specific guidance on when an agency can request completion of an SF-86 in connection with the processing of an existing security clearance that may be eligible for reciprocity. The intent is to minimize the circumstances where an SF-86 is required as part of the processing of a security clearance for reciprocity candidates.



UNCLASSIFIED//~~FOUO~~

Ms. Carrie Wibben, ONCIX/SSD's Chief, Personnel Security Group is my lead for matter. She may be reached at CARRILW2@DNI.GOV or (571) 204-6505.

Sincerely,

Michael P. Londregan

UNCLASSIFIED//~~FOUO~~

3

(U) Appendix F: Staff Acknowledgements

(U//~~FOUO~~) The following individuals made key contributions to this report:

[redacted]