

Office of the Director of National Intelligence
Washington, DC 20511

SEP - 2 2014

Mr. Steven Aftergood
Federation of American Scientist
1725 DeSales Street NW, Suite 600
Washington, DC 20036

Reference: ODNI Case # DF-2014-00193

Dear Mr. Aftergood:

This is in response to your email dated 01 May 2014 (Enclosure), received in the Information Management Division of the Office of the Director of National Intelligence (ODNI) on 01 May 2014. Pursuant to the Freedom of Information Act (FOIA), you are requesting a copy of *“Strategy and Schedule for Security Clearance Reciprocity.”*

Your request was processed in accordance with the FOIA, 5 U.S.C. § 552, as amended. One responsive document was identified (Enclosure 2), which upon review has been determined to be releasable in segregable form, pursuant to exemption (b)(3), which applies to records that, if released, would constitute a clearly unwarranted invasion of the personal privacy of individuals. The document is enclosed in this package.

If you wish to appeal our determination on this request, please explain the basis of your appeal and forward to the address below within 45 days of the date of this letter.

Office of the Director of National Intelligence
Information Management Office
Washington D.C. 20511

If you have any questions, email our Requester Service Center at DNI-FOIA@dni.gov or call us at (703) 874-8500.

Sincerely,


for Jennifer Hudson
Director, Information Management Division

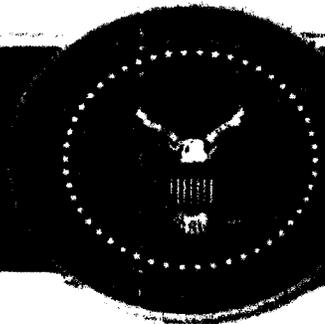
Enclosure

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Strategy and Schedule for Security Clearance Reciprocity

April 2014

LEADING INTELLIGENCE INTEGRATION



EXECUTIVE SUMMARY

The Office of the Director of National Intelligence (ODNI) is pleased to present the *Strategy and Schedule for Security Clearance Reciprocity* in response to Section 306 of the Intelligence Authorization Act (IAA) for Fiscal Year 2013.¹ This report establishes a framework for improving security clearance reciprocity across government to meet the requirements established in Section 3001(d) of the Intelligence Reform and Terrorism Prevention Act of 2004² (IRTPA).

The IAA requires a strategy and a schedule to implement the security clearance reciprocity provisions of the IRTPA. Security clearance reciprocity seeks to eliminate unnecessary background investigations and adjudications if a current investigation or adjudication exists at the same level.³ Reciprocity is the acceptance by one agency of an existing, sufficient background investigation or eligibility determination conducted previously by another authorized agency.

In his role as the Security Executive Agent, the Director of National Intelligence (DNI) directed the Office of the National Counterintelligence Executive (ONCIX) to consolidate existing reciprocity guidance based on Presidential and statutory guidance into a comprehensive national-level reciprocity policy to further promote reciprocity and improve mobility of cleared individuals.

Below is a description of the sections included in this report:

- **Process to Achieve Reciprocity** - Outlines the Security Executive Agent's strategy for accomplishing reciprocity to the fullest extent across the Executive Branch.
- **Schedule to Ensure Reciprocity** - Provides milestones by initiatives necessary to achieve consistent application of reciprocity process across the government.
- **Reciprocity Authorities and Permitted Exceptions** - Provides an overview of reciprocity related authorities and guidance issued pursuant to the reciprocity requirements directed by IRTPA.
- **Attachment - Reciprocity Memoranda** - Provides detailed guidance to agencies on reciprocity processes and permitted exceptions.

Executive Order 13467 and Reciprocal Recognition of Existing Personnel Security Clearances, ODNI Memorandum, October 1, 2008

Reciprocal Recognition of Existing Personnel Security Clearances and attached Definitions Relating to Exceptions, OMB Memorandum, November 14, 2007

Reciprocal Recognition of Existing Personnel Security Clearances (defines types of exceptions); and its attached *Checklist of Permitted Exceptions to Reciprocity*, OMB Memorandum, July 17, 2006

¹ Public.Law. No. 112-277, Intelligence Authorization Act for Fiscal Year 2013, 14 Jan 2013, Section 306, Strategy for Security Clearance Reciprocity.

² Public.Law. No. 108-458, Intelligence Reform and Terrorism Prevention Act of 2004, 17 Dec 2004, Section 3001(d), Reciprocity of Security Clearance and Access Determinations.

³ The term "security clearance" in this report applies to individuals who have actual access to classified information and those who have been approved for access, but either have not yet had a need to work with classified information, or no longer require access in the performance of their job duties, but continue to occupy sensitive national security positions.

INTRODUCTION

The executive branch has long recognized the importance of continuously improving the processes by which we determine eligibility for access to classified national security information and eligibility to occupy a national security position. In 1995, Executive Order (EO) 12968⁴ established executive branch requirements for reciprocal acceptance of access eligibility determinations between agencies and provided guidance about the conditions under which reciprocity applies. Congress strengthened reciprocity through the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), which statutorily mandated that "all security clearance background investigations and determinations completed by an authorized investigative agency or authorized adjudicative agency shall be transferable and accepted by all other agencies when a current investigation or adjudication of equal level exists to meet equivalent or less investigative or adjudicative requirements."

The Suitability and Security Clearance Reform Effort (described in the Strategic Framework submitted to Congress in February 2010) sought to improve the timeliness, efficiency, and quality of the United States Government's personnel security and suitability determinations process. EO 13467⁵ created the Performance Accountability Council, and designated the Director of National Intelligence (DNI) as the Security Executive Agent (SecEA), and the Director of the Office of Personnel Management (OPM) as the Suitability Executive Agent. The SecEA is responsible for ensuring reciprocal recognition of eligibility for access to classified information and is the final authority to resolve disputes among agencies involving the reciprocity of investigations and determinations of eligibility for access to classified information or eligibility to hold a sensitive position. As the Suitability Executive Agent, the Director of OPM is responsible for ensuring reciprocity consistent with EO 13488, entitled Reciprocity for Prior Fitness or Suitability Determinations.

This *Strategy and Schedule for Security Clearance Reciprocity* ("Reciprocity Strategy") responds to Section 306 of the Intelligence Authorization Act (IAA) for FY 2013, which directs the President to develop a strategy and a schedule to carry out the requirements of Section 3001(d) of the IRTPA to include:

- (1) A process for accomplishing the reciprocity required under such section for a security clearance issued by a department or agency of the Federal Government, including reciprocity for security clearances that are issued to both persons who are and who are not employees of the Federal Government; and
- (2) A description of the specific circumstances under which a department or agency of the Federal Government may not recognize a security clearance issued by another department or agency of the Federal Government.

This Reciprocity Strategy addresses the above requirements while outlining current initiatives that respond to findings from the December 2012 Office of the Inspector General of the Intelligence Community (IC IG) audit of IC security clearance reciprocity.

CURRENT POLICIES

In addition to EO 12968, the policies listed below were issued to ensure reciprocity of security clearance and access determinations as required by Section 3001(d) of IRTPA:

⁴ EO 12968, *Access to Classified Information*, August 2, 1995 (as amended).

⁵ EO 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*, 2008.

- a. EO 13467, *Reforming Processes Relating to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*, June 30, 2008
- b. OMB memoranda⁶ dated December 12, 2005, July 17, 2006, and November 14, 2007, subject: *Reciprocal Recognition of Existing Personnel Security Clearances*
- c. Intelligence Community Policy Guidance 704.4, *Reciprocity of Personnel Security Clearance and Access Determinations*, October 2, 2008
- d. Intelligence Community Directive 709, *Reciprocity for Intelligence Community Employee Mobility*, June 10, 2009
- e. Federal Investigative Standards, 1997 – *as amended*.⁷

Federal agencies are required to accept current and equivalent security clearance background investigations and access determinations completed by an authorized investigative or adjudicative agency, with two exceptions reflected in the OMB memorandum dated November 14, 2007:

- The gaining agency has substantial information that surfaced since the last background investigation (BI) which indicates that the individual does not or may not meet access eligibility standards or may no longer satisfy adjudicative requirements; or
- An agency used its discretion and granted or continued an existing security clearance despite a failure to meet adjudicative or investigative standards e.g. a waiver, deviation or condition⁸.

Under current policy if one of the permitted exceptions to reciprocity exists, Federal agencies may choose to reinvestigate or readjudicate the case prior to granting access.

CHALLENGES

There are several challenges to ensuring security clearance reciprocity across the Federal Government. One significant challenge has been documenting the extent to which security clearance reciprocity already occurs across agencies. Agency databases were not designed to collect metrics concerning reciprocity timeliness and effectiveness and require revision. The national security clearance database repositories (ODNI's Scattered Castles, the Office of Personnel Management's Central Verification System, and the Department of Defense's Joint Personnel Adjudication System) require modifications to capture metrics to demonstrate that reciprocity is being honored. Such modifications would permit the capability to alert clearance sponsoring agencies of any potentially adverse information that should be considered during agency adjudication deliberations or hiring decisions.

Another challenge is improving communication between acquisition and security offices. Contracting Officers (COs) and Contracting Officer Technical Representatives (COTRs) are often disconnected from security processes. As an example, security may reciprocally accept a

⁶ Former DNI McConnell's memorandum of 1 October 2008 recognized and endorsed these three OMB memoranda as DNI policy statements and reasserted the positive steps and specific actions outlined by the OMB memoranda.

⁷ The Federal Investigative Standards, as revised in 2012, will be implemented pursuant to the Federal Investigative Standards Implementation Plan, April 2014.

⁸ OMB Memorandum, 14 Nov. 2007 defines exceptions, to include conditions, waivers and deviations.

security clearance; however, COs or COTRs may incorporate a requirement for submission of an SF-86 as part of their contract requirements which may be perceived by the individual as the initiation of a new investigation or security process. CO and COTR requests for additional information or steps could result in overlapping or conflicting requirements levied on contactors thereby prolonging the security clearance approval process.

In today's fiscal environment, agencies will be challenged to fund modifications to processes and systems, collect and report data, and undergo the strict oversight and compliance required to implement new reciprocity policy. Nonetheless, the ODNI/ONCIX is committed to revitalizing efforts to define and measure reciprocity processes, publish policy, and oversee agency compliance with requirements.

WAY AHEAD

Because implementation has been inconsistent across the government, this strategy has been developed with renewed emphasis in order to standardize the conduct and measurement of security clearance reciprocity.

This emphasis on reciprocity will ensure that a common understanding of performance standards exists across executive branch agencies. Agencies will be provided timeliness standards, reporting requirements, and clarification about use of the SF-86 during reciprocal actions. Agencies will also be reminded of the circumstances when reciprocity is not required.

The ODNI/ONCIX will oversee executive branch agency processes and provide transparency into process development as well as feedback on data collection reporting. Best practices and information gained from lessons learned will be obtained and shared with agencies.

Other initiatives to improve reciprocity include research, policy, and outreach which are discussed below.

Research

The ODNI/ONCIX is conducting a Reciprocity Research Study, launched in September 2013, to examine reciprocity across the executive branch. Information obtained during site visits will help establish a baseline for how reciprocity functions, identify best practices, and determine which internal organizations – other than Security – are involved in an agency's internal processes (e.g., Human Resource and Acquisition offices).

The Reciprocity Research Study will help in designing initial data collection to refine draft reciprocity metrics currently under development. Findings from the study will also inform the creation of a reciprocity policy that will include the conditions under which additional investigative or adjudicative actions may be taken as well as conditions in which reciprocity does not apply.

In addition, the ONCIX 2013 Mission Review includes several questions which collect reciprocity data points from 18 participating agencies to inform the establishment of reciprocity performance measures as well as to baseline the current state of reciprocity. For example, the following questions were included in the Mission Review Questionnaire:

- 1) "What additional checks or other activities (i.e., polygraph, medical screening, completion of SF 86) does your agency require prior to reciprocally accepting an individual's clearance from another organization?"
- 2) "Describe your agency's approach to applying reciprocity to individuals with out-of-scope investigations more than 7 years. Does this differ based on originating agency?"

Policy

The findings from the research study and agency responses to the Mission Review Questionnaire will help inform the development of updated reciprocity policy. As appropriate, the policy will integrate guidance issued in previous documents and will specify timelines, reporting requirements, and clear definitions. The policy will be developed collaboratively with executive branch partners, and it will ensure agency awareness of requirements for reciprocal recognition of eligibility for access to classified information as well as uniformity, centralization, efficiency, effectiveness, and timeliness of agency processes.

Outreach

ODNI/ONCIX will continue to enhance its oversight and assessments program to facilitate implementation of personnel security processes and identify "best practices" and challenges that impede reciprocity. The assessment activity will include executive branch-wide agency metrics collection to provide insight into reciprocity performance.

This Reciprocity Strategy will be communicated to IC and other executive branch partners, with emphasis on collaboration with security offices involved in day-to-day security clearance reciprocity actions to inform and educate participants. The Security Clearance Reciprocity website (<http://www.ncix.gov/SEA/reciprocity.php>) will continue to be updated with new developments to educate agency representatives, cleared individuals, or other interested parties. Transparency in the reciprocity process is intended to reduce misperceptions about reciprocity activities.

The website provides information to help organizations and individuals determine if an individual's current security clearance might be reciprocally accepted. It also provides a checklist of permitted exceptions to reciprocity as provided in the OMB memoranda from December 2005 and July 2007; a list of current federal reciprocity policies; and security and suitability definitions.

SCHEDULE

Policy and guidance must be written, taking into account existing processes, decentralization of security clearance decision making, and agency-specific, mission-driven security processes. The schedule below takes into consideration the need to develop clear and consistent policies, definitions, metrics, and reporting, while obtaining, analyzing, and using information from decentralized agency-specific processes. The timelines will be monitored by the ODNI/ONCIX to ensure initiatives and actions remain on schedule.

Timeline	Actions
FY 2014, First Quarter	<ul style="list-style-type: none">• Research Team completes agency site visits for study (begun in FY 2013, fourth quarter)• Provide summary of FY 2013 agency assessments• Conduct initial data call on reciprocity• Create performance measures• Continue agency assessments• Analyze information obtained from site visits and mission review questionnaires
FY 2014, Second Quarter	<ul style="list-style-type: none">• Prepare report documenting findings of the research study

FY 2014, Third Quarter	<ul style="list-style-type: none"> • Share lessons learned and potential process improvements with agencies • Begin development of reciprocity policy
FY 2014, Fourth Quarter	<ul style="list-style-type: none"> • Issue formal performance measures data call • Begin analysis of performance metrics data • Identify agencies for follow up site visits
FY 2015	<ul style="list-style-type: none"> • Analyze performance measures data on a quarterly basis • Provide results of the performance data measures to the DNI and to individual agencies • Issue reciprocity policy

CONCLUSION

While much work lies ahead, the ODNI/ONCIX is committed to ensuring security reciprocity processes are defined, developed and delivered to the executive branch. The ODNI/ONCIX is assessing agency practices, defining measures to appraise agency performance, and educating numerous populations to eliminate confusion about reciprocity.

UNCLASSIFIED

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

[REDACTED] (b)(3)

MEMORANDUM FOR: Distribution

SUBJECT: Executive Order 13467 and Reciprocal Recognition of Existing Personnel Security Clearances

Workforce mobility is key to building an Intelligence Community as well as effective inter-agency process properly postured to meet today's global challenges and prepare for tomorrow's unknown threats. Much of that mobility rests on the inter-agency reciprocity of security clearances, especially at the Top Secret/Sensitive Compartmented Information level.

As the Security Executive Agent, I remain committed to streamlining the process by which we determine eligibility for access to Classified National Security Information. Executive Order (EO) 13467, signed in June 2008, provides for major changes to the government's personnel security programs. The EO directs the alignment of existing processes for eligibility for access to classified information and security clearances using consistent standards. Specifically, it calls for reciprocal recognition while ensuring cost-effective, timely, and efficient protection of the national interest.

We will manage a forthcoming policy process that will ensure we make the changes envisioned by the EO. The attachments contains our specific policy statements on several of the reciprocity issues and reasserts the positive steps and specific actions outlined in three executive memoranda issued by the Office of Management and Budget over the last three years.

We welcome your assistance and input on this matter. If you have any questions, please direct them to Mr. Fitzpatrick, our Director of the Special Security Center. He can be reached at 703-482-5106.



J. M. McConnell

1 OCT 08

Date

Attachments:

1. DD/OMB Memorandum, dtd 12 December 2005 with DNI Endorsement.
2. DD/OMB Memorandum, dtd 17 July 2006 with DNI Endorsement.
3. DD/OMB Memorandum, dtd 14 November 2007 with DNI Endorsement.

UNCLASSIFIED

UNCLASSIFIED

SUBJECT: Executive Order 13467 and Reciprocal Recognition of Existing Personnel
Security Clearances

External Distribution:

Secretary of Agriculture, Department of Agriculture
Secretary of Commerce, Department of Commerce
Secretary of Defense, Department of Defense
Secretary of Education, Department of Education
Secretary of Energy, Department of Energy
Secretary of Health and Human Services, Department of Health and Human Services
Secretary of Homeland Security, Department of Homeland Security
Secretary of Housing and Urban Development, Department of Housing and Urban Development
Secretary of the Interior, Department of the Interior
Attorney General, Department of Justice
Secretary of Labor, Department of Labor
Secretary of State, Department of State
Secretary of Transportation, Department of Transportation
Secretary of the Treasury, Department of the Treasury
Secretary of Veterans Affairs, Department of Veterans Affairs
Director, Central Intelligence Agency
Director, Defense Intelligence Agency
Director, Office of Intelligence and Counterintelligence, Department of Energy
Under Secretary, Intelligence and Analysis, Department of Homeland Security
Assistant Secretary, Bureau of Intelligence and Research, Department of State
Assistant Secretary, Intelligence and Analysis, Department of Treasury
Chief of Intelligence/Senior Officer (SOIC), Drug Enforcement Administration
Executive Assistant Director, National Security Branch, Federal Bureau of Investigation
Director, National Geospatial-Intelligence Agency
Director, National Reconnaissance Office
Director, National Security Agency
Deputy Chief of Staff, G2 Army
Director of Naval Intelligence, United States Navy
Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance, United States Air Force
Director of Intelligence, Headquarters, U.S. Marine Corps
Assistant Commandant for Intelligence and Criminal Investigations, United States Coast Guard



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

DEPUTY DIRECTOR
OF MANAGEMENT

November 14, 2007

MEMORANDUM FOR DEPUTIES OF EXECUTIVE DEPARTMENTS AND
AGENCIES

FROM: Clay Johnson III
Deputy Director for Management

SUBJECT: Reciprocal Recognition of Existing Personnel Security Clearances

The OMB memoranda of December 12, 2005, and July 17, 2006, on this same subject indicated that there are only two authorized exceptions to reciprocity if an individual has a current access eligibility determination based upon the requisite investigation in terms of scope and currency. One is when an agency used its discretion and decided to grant or continue the existing security clearance for an individual despite a failure to meet adjudicative or investigative standards. The other is when the gaining program or organization is already in possession of substantial information indicating that, notwithstanding the existing clearance, the adjudicative standards may not be satisfied in light of the new information. In both instances, other agencies are allowed to reinvestigate or readjudicate the case prior to granting another security clearance.

Successful implementation of these two limited exceptions to reciprocity requires a consistent understanding of what constitutes a condition, waiver or deviation as well as what constitutes substantial issue information. To that end, the Personnel Security Working Group of the Records Access and Information Security Policy Coordinating Committee has adopted the attached definitions relating to exceptions to reciprocity to be used by all agencies when making an access eligibility determination.

These instructions are issued pursuant to the authority of the Director of the Office of Management and Budget under section 2 of the Executive Order 13381, "Strengthening Processes Relating to Determining Eligibility for Access to Classified National Security Information," as amended, and subject to section 5(a) of that order, and are effective immediately.

Attachment

Definitions Relating to Exceptions

EXCEPTION. An adjudicative decision to grant or continue access eligibility despite a failure to meet adjudicative or investigative standards. The head of the agency concerned or designee will make such decisions. (Exceptions with regard to eligibility for Sensitive Compartmented Information (SCI) will be processed according to procedures established by the Director of National Intelligence (DNI).) For purposes of reciprocity, the presence of an exception permits the gaining organization or program to review the case before assuming security sponsorship and to accept or decline sponsorship based on that review. When accepting sponsorship, the gaining organization or program will ensure that the exception remains a matter of record. There are three types:

1. **CONDITION.** Access eligibility granted or continued with the proviso that one or more additional measures will be required. Such measures include additional security monitoring, restrictions on access, and restrictions on an individual's handling of classified information.
2. **DEVIATION.** Access eligibility granted or continued despite a significant gap in coverage or scope in the supporting background investigation. "Significant gap" for this purpose means either complete lack of coverage for a period of six months or more within the most recent five years investigated or the lack of an FBI name check or an FBI fingerprint check or the lack of one or more investigative scope requirements in its entirety (e.g., the total absence of local agencies checks within an investigation would constitute a deviation, but the absence of local agencies checks for some but not all places of residence would not constitute a deviation).
3. **WAIVER.** Access eligibility granted or continued despite the presence of substantial issue information that would normally preclude access. Agency heads or designees approve waivers only when the benefit of access clearly outweighs any security concern raised by the shortcoming. A waiver may require special limitations on access, additional security monitoring, and other restrictions on the person's handling of classified information beyond normal need-to-know.

ISSUE INFORMATION. Any information that could adversely affect a person's eligibility for classified information. There are two types:

MINOR ISSUE INFORMATION. Information that meets a threshold of concern set out in "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information," but for which adjudication determines that adequate mitigation, as provided for by the Guidelines, exists. Minor issue information does *not* provide the basis for a waiver or condition.

SUBSTANTIAL ISSUE INFORMATION. Any information, or aggregate of information, that raises a significant question about the prudence of granting access eligibility. Substantial issue information constitutes the basis for granting access eligibility with waiver or condition, or for denying or revoking access eligibility.



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

DEPUTY DIRECTOR
FOR MANAGEMENT

M-06-21

July 17, 2006

MEMORANDUM FOR DEPUTIES OF EXECUTIVE DEPARTMENTS AND AGENCIES

From: Clay Johnson III
Deputy Director for Management

Subject: Reciprocal Recognition of Existing Personnel Security Clearances

The OMB memorandum of December 12, 2005, on this same subject, outlined the various issues that inhibit reciprocity of security clearances and the actions required to address them. Since then, it has become apparent that additional actions are required to further reciprocity with respect to special access programs (SAPs). In that vein, paragraph 3(d) of the referenced memorandum is revised as follows:

- (d) **Required Action: While Executive Order 12968 allows agency heads to establish additional but not duplicative investigative or adjudicative requirements for SAPs (including SCI) or for detail or assignment to their agencies, agencies will limit such additional requirements to the following:**
- **Administering polygraph examinations.**
 - **Disqualifying individuals based upon non-U.S. immediate family members.[†]**
 - **Requiring personnel security investigations completed within seven years irrespective of the classification level of the SAP. The requirement to submit the Periodic Reinvestigation packet NLT the 5th year anniversary remains unchanged.**

In lieu of the polygraph, agencies may require personnel:

- **Seeking initial access to a SAP at each agency[‡] (or access to a SAP at a higher classification level than a SAP currently accessed) to submit a current SF 86 (defined as completed and signed within the last year).**
- **Already accessed to a SAP to submit an updated and signed SF 86 or a SF 86C on an annual basis.**

The Checklist of Permitted Exceptions to Reciprocity, provided with the referenced OMB memorandum, is revised to reflect the above and is attached.

^{*} That is, special access programs in the specific sense of EO 12958, sec. 4.4.

[†] Other than this one exception, access eligibility determinations for SAPs will be made in accordance with national adjudicative guidelines.

[‡] For purposes of reciprocity, all components of the Department of Defense to include the Military Departments and Defense Agencies shall be considered one agency.

Any agency head who determines that it is necessary to impose additional requirements, other than the above, for the purpose of determining eligibility for access to classified information will notify the Director of OMB.

Agencies will make SAP access eligibility determinations with the goal of making 80% of all determinations within 30 days.

The Records Access and Information Security PCC will initiate action to formalize the above change in existing policy documents.

Attachment

Checklist of Permitted Exceptions to Reciprocity

(to be used whenever you make an eligibility determination for access to classified information for an individual who has a current access eligibility based upon the requisite investigation (i.e. ANACI, NACL, SSBI, or SSBI-PR))

For the purpose of determining eligibility for access to classified information, to include highly sensitive programs (i.e. SCI, SAPs and Q), as the gaining activity/program for an individual who has current access eligibility with another Federal agency or program:

- you cannot request the individual to complete a new security questionnaire;
- you cannot review existing background investigations for the individual;
- you cannot review existing security questionnaires for the individual;
- you cannot initiate any new investigative checks;

unless one or more of the questions below can be answered in the affirmative.

	Yes	No	N/A
1. Is the existing clearance granted on an interim or temporary basis?			
2. Is the investigation upon which the existing clearance is based more than seven years old for TOP SECRET, ten years old for SECRET and fifteen years old for CONFIDENTIAL? (See Note 1)			
3. Is your activity (i.e. the gaining activity) aware (i.e. already in possession) of substantial information indicating that the standards of E.O. 12968 may not be satisfied?			

If the individual is being considered for access to a highly sensitive program (i.e. SCI, SAP or Q) at your activity:

4. Is the existing access eligibility determination based upon a waiver or deviation, or is access otherwise subject to conditions?			
5. If applicable, does the individual not satisfy a polygraph requirement imposed by the new program, as approved by the agency head or deputy? (See Note 2)			
6. If applicable, does the individual not satisfy a requirement imposed by the new program that prohibits any non-U.S. immediate family or non-U.S. cohabitants, as approved by the agency head or deputy? (See Note 2)			
7. For SAP access, is this the individual's initial consideration for a SAP access eligibility determination (i.e. the individual does not have a current access eligibility determination at the same or higher classification level with the same agency)? (See Notes 3, 4 & 5)			
8. For SAP access where the individual has current SAP access, has the individual failed to submit a certification of a prior security questionnaire or an updated SF 86C as required within the past year? (See Notes 3, 4 & 5)			

Items 1 and 2 and 4 through 6 above can be verified by querying OPM's Clearance Verification System (CVS), the Department of Defense's Joint Personnel Adjudication System (JPAS), or the Intelligence Community's Scattered Castles database. If you do not have on-line access to the appropriate database, or if the record is otherwise incomplete, you can fax an "Inter-Agency Clearance Verification Request" to the appropriate agency. The request form and appropriate fax numbers can be found at:

<https://opmis.xsp.org>

Note 1 – An investigation for SAP access will be considered current if it is no more than five years old (seven years old if a periodic reinvestigation was submitted prior to expiration of the investigation and is currently pending), regardless of the classification level.

Note 2 – Under such circumstances, only additional – not duplicative – investigative or adjudicative procedures will be completed.

Note 3 – For purposes of reciprocity, all components of the Department of Defense to include the Military Departments and Defense Agencies shall be considered one agency.

Note 4 – Under such circumstances, a current SF86, an SF 86C, or pen/ink changes to an existing SF 86 can be required.

Note 5 – You can review an existing background investigation for the individual and/or request an investigative check only if the SF 86 or SF 86C contains new substantive information of security concern not previously considered in the prior SAP access eligibility determination or the last security clearance adjudication and could serve as the basis for disqualification. New substantive information will be adjudicated by a CAF in accordance with national adjudicative guidelines.