

REPORT OF
THE SECURITY CLEARANCE OVERSIGHT GROUP
CONSISTENT WITH
TITLE III OF THE INTELLIGENCE REFORM AND TERRORISM
PREVENTION ACT OF 2004



FEBRUARY 2007

Executive Summary

Government agencies are making significant progress determining security clearance eligibility as called for by the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). Current investigative and adjudicative timeliness for 80% of the requests for initial clearances is generally as called for by IRTPA: 90 days or less for investigations and 30 days or less for adjudications.

- For requests for initial security clearances from agencies served by OPM (90% of total clearances), we project that the average time for investigations for 80% of initial clearances begun after October 1, 2006, plus the average time for adjudications for 80% of adjudications begun and reported after October 1, 2006, will be 120 days or less.
- 80% of the initial clearance investigations performed by OPM, completed after October 1, 2006, averaged 101 days, while 80% of the adjudications by those agencies whose investigations are performed by OPM, completed and recorded after October 1, 2006, averaged 17 days. The combined averages for investigations and adjudications averaged 118 days for 80% of those completed after October 1, 2006.
- ALL investigations completed by OPM after October 1, 2006 averaged 166 days, while ALL adjudications completed and reported by agencies whose investigations are done by OPM, averaged 39 days; so the total of the two averages is 205 days.

However having investigative timeliness and adjudicative timeliness for initial clearances at the levels called for by IRTPA does not mean we are most assuredly granting security clearances as quickly as desired or called for.

- Reinvestigation timeliness has not been addressed, because the improvement effort focused on individuals for whom initial security clearances are required to perform work.
- Not included is the time to hand-off applications to the investigative agency, hand-off investigation files to the adjudicative agency, return the files to the investigative agency for further information, if necessary, and/or generally complete the security clearance process within the agency, once the investigation and adjudication are complete.
- Some of the performance information referenced in this report is necessarily for just a few months of activity; so we need to perform at the desired levels for longer periods of time for the information to be considered representative of what Industry and Agency employees can expect.

Background

Presently, the Federal government processes approximately 1.9 million requests for background investigations each year to support determinations of an individual's suitability for employment or eligibility for access to classified information, or fulfill agencies' other regulatory requirements. The average time to conduct the investigation had been about one year for Top Secret clearances and 5 to 6 months for Secret/Confidential, a totally unacceptable length of time.

		FY 04	FY 05
Initial Clearance Investigations Completed	Top Secret <i>Average Days</i>	392 days	347 days
	Secret/Confidential <i>Average Days</i>	179 days	155 days
Reinvestigations for Top Secret Completed	<i>Average Days</i>	579 days	482 days

To increase attention to and accountability for the timeliness and continued quality of the investigations and adjudications required to grant these clearances, IRTPA included the following language:

During the period beginning on a date not later than... [December 2006], each authorized adjudicative agency shall make a determination on at least 80 percent of all applications for a personnel security clearance pursuant to this section within an average of 120 days after the date of receipt of the application for a security clearance by an authorized investigative agency. Such 120-average period shall include-

- (i) a period of not longer than 90 days to complete the investigative phase of the clearance review; and*
- (ii) a period of not longer than 30 days to complete the adjudicative phase of the clearance review.*

As called for by IRTPA, the President designated OMB to lead a task force of the major clearance granting agencies, including the intelligence community and the investigations service providers, to identify areas of responsibility, establish performance requirements, and help hold agencies accountable for doing what they said they would do to improve the security clearance process. This oversight group's plan to reform the process, submitted to Congress on November 9, 2005, was to:

- Increase agencies' commitment to and accountability for their part of the security clearance granting process, with clearer goals for each part of the process and regular, transparent performance information relative to those goals;
- Expand investigative capacity at OPM where 90% of the investigations are conducted and rely initially on currently approved investigation methodologies;
- Have OPM help the record repositories (FBI, DOD, DOS, etc.) identify and resolve impediments to timeliness, apply additional resources to the reduction of the backlog of old file requests, and establish work plans to achieve and maintain acceptable timeliness;
- Expand adjudicative capacity as appropriate at every adjudicating agency and rely initially on currently approved adjudication methodologies;
- Adopt and utilize currently available electronic file transfer capabilities to lessen the time to initiate an investigation and an adjudication;
- Focus first on initial investigations versus reinvestigations;
- Establish the reciprocal acceptance of security clearances granted by other agencies, called for by EO 12968 and National Security Directive 63, which agencies have never been held accountable for implementing;
- Focus initially on work done by OPM and its client agencies; and
- Organize a research and development effort to identify investigation and adjudication methodologies for the future and employ new techniques if research shows they improve the quality and/or timeliness of the security clearance granting process.

All agencies have made improving the security clearance granting process a priority. Industry counsel on the reform efforts has been solicited monthly, and industry and Congress have been kept up-to-date on agency progress.

Performance

IRTPA calls for the average number of processing days for 80% of security clearance requests submitted at the end of 2006 to be 90 days or less for the investigation and 30 days or less for the adjudication.

Looking at initial investigations and adjudications initiated after October 1, 2006, for the clearance requests with the investigations performed by OPM:

- As of February 3, 2007, 64% of the 49,633 initial clearance investigations initiated by OPM during October 2006 have been completed. Average processing time for these is 63 days, and at the current rate of processing, we project 80% will be completed in an average of 90 days or less. Forty-four percent of the 6,366 requests for Top Secret level investigations have been

completed in an average of 75 days, and 67% of the 43,267 investigations for Secret/Confidential level have closed in an average of 61 days.

- For 37,412 initial clearance investigations that were completed and forwarded to agencies for adjudication in October 2006, 71% have been reported as adjudicated in an average of 23 days. We project 80% will be completed in an average of 30 days or less.
- DOD (92% of total adjudications) has reported adjudications on 72% of their investigations completed in an average of 23 days. Non-DOD agencies have reported adjudication on 60% of their investigations completed in an average of 22 days.

Looking at ALL initial investigations and adjudications completed after October 1, 2006 (regardless of the date of submission), for the clearance requests with the investigations done by OPM:

- 80% of the 154,716 initial investigations completed by OPM during the 1st quarter of FY 07 averaged 101 days in process. The difference between the timeliness of these investigations versus those requested and completed after October 1, 2006 (63 days; see above) reflects the large number of aged investigations that were completed during this period, with the help of the additional resources being applied to the process and the more timely retrieval of required documents and files.
- ALL investigations completed by OPM in FY 07 for initial clearances averaged 166 days. The average initial security clearance investigation took 205 days in 2004, 188 days in 2005, and 176 in 2006.
- Overall, OPM is making significant progress reducing the backlog of aged investigations. In February 2006, OPM's pending case inventory included over 62,000 investigations (of all types, including reinvestigations) that were over one year old. As of February 3, 2007, that number was reduced to 48,163 investigations pending in process more than one year. Of these, OPM has completed all required basic coverage for over 27,000 that are now awaiting third-party records and/or a special subject interview to address issues developed during the investigation.
- For 117,054 initial adjudications completed and recorded during the first quarter of FY 07, 80% averaged 17 days to process, while the average time for all was 39 days.
- DOD (93% of this activity) averaged 18 days for 80% of the 108,903 actions reported, and Non-DOD agencies averaged 15 days for 80% of the 8,151 actions they reported.

While reinvestigations were not the focus of the reform effort in FY 06, OPM will focus on achieving mutually acceptable timeliness standards for this critical workload in FY 07 and beyond.

- 80% of all completed reinvestigations in the first quarter of FY 07 averaged 279 days in process. As discussed later, reinvestigation timeliness will be a focus of the reform effort in 2007.

The reform effort focused on investigation and adjudication timeliness for the clearance determinations for which OPM conducts the investigations. As part of our Security Clearance Oversight Team, however, the Intelligence Community and those agencies with a delegation to conduct their own investigations (e.g., Justice, DHS, and DOS) have also been working toward meeting the IRTPA standards.

- For the Intelligence Community, 83% of all investigations and adjudications completed in FY 06 and the 1st quarter of FY 07 were completed in an average of 103 days (investigation and adjudication time combined).
- The State Department completed 83% of 4,143 investigations initiated in the 4th quarter of FY 06 in an average of 47 days and adjudicated 100% of its completed investigations in an average of 4 days.
- The Department of Homeland Security (DHS) is developing data reporting mechanisms to track clearance determinations with the same level of data detail provided by OPM. For those investigations and adjudications for headquarters and the Immigration and Customs Enforcement agency (ICE), DHS reports that as of January 30, 2007, 72% of the 245 investigations initiated in October 2006 are complete with 36% of their adjudications completed within 30 days.
- The Department of Justice/FBI completed 39% of 2,230 initial investigations completed in the 1st quarter of FY 07 within 90 days, with an overall average of 146 days in process. Eighty-nine percent of its adjudication actions were completed within 30 days, with an average processing time of 11 days. In general, FBI continues to address its pending inventory on a first-in, first-out basis.

It should be noted that not all Intelligence Community elements have delegated investigative authority; those that do not utilize OPM for their investigations.

Status of Initiatives Supporting Improved Performance

OPM

A critical factor in meeting the goals of the IRTPA was increasing the investigative capacity through the addition of new staff (Federal and contractor) at OPM. In the November 2005 plan, OPM estimated that 8,000 full time staff, working at a normal performance level, were required to handle annual workload projections. Additional resources were needed to eliminate the backlog and offset newer staff working at a

less than full performance level. OPM has steadily increased staffing levels and both the Federal and contractor staffs are performing as planned:

March 2005:	7,819 total Staff (5,868 field staff)
March 2006:	8,590 total Staff (6,505 field staff)
January 2007:	9,367 total Staff (7,312 field staff)

During this period of extreme growth, OPM has developed additional internal quality control processes to ensure that the quality of completed investigations continues to meet the national investigative standards. Overall, less than 1% of all completed investigations are returned to OPM from the adjudicating agencies for quality deficiencies.

Availability of Federal Records: FBI

In June 2006, the FBI and OPM entered into a Memo of Agreement (MOA) to reduce the number of OPM name check requests pending in excess of 30 days to a level that is in compliance with guidance promulgated by OPM pursuant to the IRTPA.

- To add to the existing FBI name check staff, OPM provided 32 staff and the FBI devoted an additional 30 staff to this effort. The project started with 69,450 security related OPM name check requests pending for over 30 days. Of those original name check requests, 85% have been completed as of February 2, 2007. Currently, 45,192 OPM name check requests remain pending for greater than 30 days. In FY 06, OPM submitted 1,293,754 name checks to the FBI.
- The FBI and OPM are working together to automate the exchange of information to reduce processing time.
- Additional FBI/OPM process enhancements and technology improvements are also underway. As fee adjustments are finalized to ensure adequate funding, and the FBI continues to automate its processes, the backlog will be eliminated.

Availability of Federal Records: Other

Checks of State Passport records are now conducted electronically, reducing the turnaround time from 90-110 days to 17 days on average.

Searches of military service records are being made available electronically. Air Force and Army records became available in 2005, while the Navy records will be available in early 2007.

Law enforcement checks are now electronically available for Alabama, Virginia, Maryland, South Carolina, Texas, New York and New Hampshire. As OPM

conducts in excess of three million law searches each year, it is critical that it have electronic access to the law enforcement records when available in other states.

Overseas Investigations

OPM sent 177 agents abroad in 2006 and closed more than 15,000 international leads. It has made arrangements with DOS to train and use DOS eligible family members as independent investigative contractors, and has created the International Investigations Unit to better manage and track the workload.

Reciprocity

Mutually agreed upon standards for reciprocal recognition of security clearances were issued by the Administration in December 2005. Additional standards were issued in July 2006 to address unique challenges represented by special access programs due to their extra sensitivity. Copies of both memoranda are included in the appendix. In addition, the following steps have been taken to help ensure clearance reciprocity:

- An interagency collaboration forum was established to increase familiarity with processes, procedures, and issues as well as to build confidence in each other's clearance adjudicative decisions;
- Personnel Security Reciprocity Reviews were conducted at all agencies with a sizable number of cleared personnel in order to identify inconsistencies in application of policy and to provide a mechanism for resolution;
- A uniform program of instruction for agency adjudicative personnel was developed and promulgated, including core content and learning objectives, in order to further consistent clearance decisions from agency to agency; and
- A monthly sampling process was established in collaboration with a number of industry associations that represent companies that perform on classified contracts with the government, in order to assess progress in meeting reciprocity standards.

Based upon feedback from industry and other sources, we recognize that many perceived failures in clearance reciprocity actually stem from the varied standards employed by agencies to determine suitability for employment or suitability for access to unclassified spaces and information systems. We have initiated efforts to reconcile suitability and clearance eligibility standards to the extent practicable.

Use of eQIP

Electronically submitting the information required for a security clearance investigation reduces the overall time to get a clearance two to three weeks at a

minimum. Although the eQIP electronic application has existed since 2003, agencies were only held accountable for using it starting in January 2006. Overall use of the form has increased dramatically, and DOT and DOC and several small agencies are currently meeting the goal of 100% eQIP usage.

Percent of Investigations Submitted Using eQIP	1st Qtr, FY06	1st Qtr, FY07	January 2007
All Agencies	34%	65%	64%
DOC	7%	100%	100%
DOD	36%	65%	69%
DOE	0%	68%	79%
DHS	6%	64%	63%
DOJ	0%	60%	94%
DOT	74%	100%	100%

All agencies that use eQIP plan to achieve 100% eQIP usage in FY 07.

R&D

In support of the Security Clearance Oversight Committee, the Office of the Director of National Intelligence has organized an R&D subcommittee, with membership from across the Executive Branch. The subcommittee's goal is to establish and execute a national personnel security research agenda to identify the new standards and methodologies that will be necessary for timeliness to be reduced to 40 days for investigation and 20 days for adjudication. The priority areas for research are:

- Electronic transmission of all related records
- Revalidation of all investigative standards and adjudication guidelines
- Utility of internet and/or other commercially available data sources
- Opportunities to increase the integrity of the applicant interview
- Opportunities to better assess an applicant's allegiance
- Opportunities to prescreen prospective applicants
- Opportunities to get more candid information from an applicant's supervisor
- An automated tool to assist with adjudicative decisions

Timetables will be agreed to in the next month and research will begin thereafter. The agenda will include short and long-term projects that involve both public and private sector resources, including: internal ODNI resources, the Department of Defense's Personnel Security Research Center (PERSEREC), as well as academic and commercial entities with relevant expertise.

Automated Continuing Evaluation

PERSEREC is conducting a pilot test for DHS of the Automated Continuing Evaluation System (ACES) that it developed for DOD. DHS plans to employ ACES between periodic reinvestigations and as a risk management tool during individuals' employment. This tool, combined with the Phased Periodic Reinvestigation for Top Secret clearances, has the potential for providing critical information between reinvestigation cycles while reducing the labor intensive field coverage required in a full-scope reinvestigation.

Industry Feedback

Clearance processing times are especially critical to companies that perform on classified contracts with the government and most companies track them. As recently as September 2006, representatives of industry reported that access eligibility determinations based upon an initial Single Scope Background Investigations (SSBI) for their employees reflected an average end-to-end completion in excess of a year. A working group comprised of representatives of both government and industry recently conducted an end-to-end audit of a limited sample of initial SSBI industry cases that were posted as adjudicated in September 2006. This audit confirmed that the average end-to-end processing time for these cases was consistent with industry's reported experience.

Since approximately two-thirds of the cases were part of a longstanding backlog and the investigations were initiated before 2006, the lengthy investigative times were not entirely unexpected. As the backlog declines, overall end-to-end processing times will continue to improve. The adjudicative times for the audited cases, being more recent, were within the current 30-day goal.

Nonetheless, the audit revealed the need for continued process improvements and the creation of a case life-cycle tracking system, at least for industry, to encompass end-to-end metrics so as to better reflect actual experience. Specific areas requiring continued attention include:

- The time between when an industry employee is authorized to begin completion of the personnel security questionnaire (PSQ) and it is accepted by Defense Industrial Security Clearance Office (DISCO), a component of the Defense Security Service that serves as the central clearance authority for industry.
- The time it takes for the PSQ to be processed and forwarded by DISCO and scheduled for investigation by OPM.
- The time it takes for the investigative results to be forwarded by OPM and received by DISCO.

- The additional elapsed time when a completed investigation does not result in a clearance eligibility determination for various reasons, to include the need for additional investigative activity, loss of jurisdiction, transfer of adjudicative responsibility to another Central Adjudication Facility (CAF) or due process considerations.
- The additional time it takes when a completed case is forwarded to another CAF for adjudication of Sensitive Compartmented Information access.

As a result of this study, OPM and DOD will develop and institutionalize a comprehensive system of metrics, to include key data points such as those described above, to measure timeliness of the end-to-end clearance process for industry.

Priority Challenges/Opportunities to Be Addressed

Non-legislative

OPM investigation timeliness is impacted by the fact that record repositories, especially FBI, must continue to apply additional resources to get and stay current (i.e., provide 90% of the requested files within 30 days).

Legislative and Legal

OPM investigation timeliness is impacted by the fact that:

- Many state and local agencies (such as California Department of Justice) restrict access to their records, charge OPM unreasonable fees, or fail to respond to requests in a timely manner;
- OPM-FISD is not recognized as a criminal justice agency. Therefore it is often denied access to Criminal History Record Information (CHRI) that would normally be released to other agencies with criminal justice components (i.e., the FBI, CIA, DOD, etc.);
- In some jurisdictions, Federal contractors are not considered under the term “covered agency” for the purpose of conducting federal investigations, thus making agencies reluctant to release CHRI to OPM contractors. Contractors have been denied access to CHRI because they are considered as “businesses for profit” and are charged fees as if they are representing private investigative agencies;
- OPM-FISD lacks the full authority and protections to operate internationally when conducting Federal background investigations;
- Private employers are reluctant to cooperate with OPM investigators without a “hold harmless” clause to shield employers and their employees from providing information to OPM.

Goals for December 2007, in light of December 2009 goals

As stated above, new investigation methodologies must be identified to achieve the 2009 IRTPA goals, especially the 40-day timeliness goal for investigations. As the likely impact of potential new methodologies will not be known until the end of 2007 and/or beyond, it is premature to establish performance goals for 2008, and determine if the December 2009 goals are achievable and in the best interest of national security.

In general in 2007, we think our appropriately aggressive goals should be to:

- Clearly and consistently perform at slightly better than the 12/06 IRTPA goal level,
- Ensure we are reforming the entire security clearance granting process, beyond just the time it takes to conduct the investigations and adjudications.

More specifically we will hold ourselves accountable for accomplishing the following for 12/07:

- 85% of initial clearance investigations completed within an average of 90 days;
- Priority processing (less than 40 days on average) will be available for up to 10% of initial investigations;
- 80% of reinvestigations completed within an average of 180 days;
- Priority processing (less than 40 days on average) will be available for up to 10% of reinvestigations; and
- 80% of adjudications completed within an average of 25 days.

And supporting these performance targets:

- Participating agencies will achieve 100% eQIP usage, with submission of all required data and forms for investigation within 14 days or less from the date the subject provides all required material. Less than 5% of all submissions will be rejected due to errors in submission.
- With the help of OPM, the record repositories will achieve the goal of producing 90% of the requested files/information in 30 days or less.
- OPM will develop the capacity to electronically transmit completed investigations and agencies will develop parallel systems to receive completed investigations electronically, eliminating mail and handling time.
- Agencies will measure and report additional adjudicative time required to process clearances when access to SCI or SAP information is involved.
- OPM and DOD will measure timeliness of the end-to-end clearance process for industry and develop and implement necessary process improvements.
- Agencies and OPM will develop additional measures of investigation quality, if possible.

Appendix

1. Security Clearance Investigation Processing – Agency Performance Report
2. December 12, 2005 Memorandum on Reciprocal Recognition of Existing Personnel Security Clearances
3. July 17, 2006 Memorandum on Reciprocal Recognition of Existing Personnel Security Clearances
4. Title III of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law No: 108-458)

Security Clearance Investigation Processing - Agency Performance Report

Clearance Granting Agencies <i>Listed in order of total volume of National Security Investigations</i>	Total Investigations Requested All Types <i>(Suitability & Security)</i>	SF 86 Submissions National Security Initial and Reinvestigations <i>Goal: Actual submissions within 5% of projections *</i>		% Submitted Via eQIP <i>Goal: 100%</i>		% Deficient Submissions <i>Goal: Less than 5%</i>		Submission Timeliness - Hardcopy <i>Goal: Less than 14 Days</i>		Submission Timeliness - eQIP <i>Goal: Less than 14 Days</i>		Average Days for All Adjudication Actions Reported** <i>Goal: 80% Average 30 days or less (45 days including mail/handling)</i>
		FY 06	FY 07	FY 06	FY 07	FY 06	FY 07	FY 06	FY 07	FY 06	FY 07	
(Entire FY 06 - 1st Qtr FY 07)												
Defense	1,053,946	650,136	160,460	43%	65%	13%	12%	30 days	29 days	13 days	12 days	52 days
Homeland Security	100,543	25,789	6,701	33%	64%	11%	7%	34 days	36 days	60 days	33 days	74 days
Energy	22,112	18,878	4,789	27%	69%	15%	7%	36 days	42 days	28 days	31 days	72 days
Justice	21,274	5,465	1,300	14%	62%	11%	8%	38 days	40 days	20 days	33 days	158 days
OPM	7,895	4,430	1,173	87%	96%	0%	1%	24 days	11 days	11 days	7 days	28 days
Transportation	17,034	1,845	337	84%	100%	7%	3%	34 days	n/a	29 days	19 days	71 days
NRC	3,158	1,238	335	88%	86%	4%	3%	30 days	37 days	30 days	36 days	97 days
Interior	21,432	1,017	204	5%	16%	17%	21%	36 days	36 days	16 days	15 days	96 days
Treasury	87,369	966	132	17%	22%	26%	32%	36 days	46 days	16 days	18 days	90 days
DHHS	33,998	808	382	41%	91%	27%	29%	54 days	40 days	52 days	50 days	69 days
Commerce	15,823	594	173	57%	100%	6%	5%	37 days	n/a	19 days	16 days	54 days
Agriculture	12,807	553	116	94%	100%	2%	4%	66 days	n/a	46 days	30 days	72 days
NASA	6,744	526	150	91%	100%	2%	1%	36 days	n/a	22 days	21 days	112 days
EPA	3,370	212	69	76%	99%	7%	5%	52 days	8 days	29 days	19 days	71 days
NARA	2,162	146	15	96%	100%	4%	5%	24 days	n/a	28 days	29 days	70 days
VA	158,954	119	13	48%	77%	9%	6%	43 days	27 days	31 days	54 days	85 days
GSA	3,403	103	55	20%	25%	4%	4%	54 days	48 days	54 days	43 days	42 days
Labor	1,792	74	19	1%	63%	32%	6%	33 days	120 days	7 days	17 days	66 days
HUD	1,874	72	15	3%	14%	14%	14%	21 days	30 days	28 days	13 days	84 days
Education	4,671	67	12	81%	100%	7%	10%	24 days	n/a	27 days	19 days	83 days
FCC	784	64	13	99%	100%	0%	0%	14 days	n/a	13 days	8 days	134 days
NSF	1,030	19	8	89%	100%	20%	0%	26 days	n/a	18 days	19 days	94 days

* Workload Projection Goals: Goal not met for FY 06. FY 07 submissions, by agency, are being monitored monthly.

** Ajudication time posted is for all reported actions and includes mail/handling time, estimated up to 15 days, between OPM and adjudicating agency




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

DEPUTY DIRECTOR
FOR MANAGEMENT

December 12, 2005

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 Federal government is committed to significantly improving the process by which we determine eligibility for access to Classified National Security Information. This commitment is reinforced by requirements to improve the security clearance process included in Title III of Public Law 108-458 (The Intelligence Reform and Terrorism Prevention Act of 2004) and Executive Order 13381 (Strengthening Processes Relating to Determining Eligibility for Access to Classified National Security Information). A significant part of this reform is ensuring that background investigations are conducted to grant new security clearances only when they are actually required.

The attached paper outlines the various issues currently inhibiting reciprocity of security clearances, and the actions you and others are required to take to address them. **Your department or agency, and all others, are responsible for the actions highlighted in bold.**

This reciprocity guidance was developed by a Security Clearance Oversight Steering Committee, which includes representatives from DoD, DHS, DOE, DOJ, DOT, DOC, DOS, the DNI, the NSC, and the National Archives and Records Administration. I am the Chairman.

If you have any questions about the requirements contained in this document, please contact me at (202) 456-7070.

cc: Departments and Agencies Directors of Security

Enforcing Reciprocity of Existing Personnel Security Clearances

1. **Issue:** There is an inconsistent understanding among the agencies with respect to when reciprocal recognition of an existing clearance is required.
 - (a) **Required Action:** The **attached checklist** is designed to assist agencies in determining when reciprocal recognition of existing clearances is required and **should be used whenever applicants indicate that they possess an existing access eligibility determination at the same or higher level than currently needed.**
2. **Issue:** The existing central database does not provide sufficient clearance verification information on a real-time basis to enable agencies to ascertain the status of an individual's security clearance.
 - (a) **Required Action:** OPM has added additional data fields to the Clearance Verification System (CVS) so as to differentiate between those access eligibility determinations that require reciprocal recognition and those that do not (see attachment 2 for required data fields and explanation). These additional fields will be fully incorporated in CVS by December 17, 2005.
 - (b) **Required Action:** While agencies are migrating to CVS, OPM will develop and promulgate guidance that directs agencies to: i) query DoD's JPAS database if the existing clearance was issued by a DoD activity; ii) query the Intelligence Community's Scattered Castles database if the existing clearance was issued by an intelligence community agency; or iii) query the appropriate agency via phone or fax using a comprehensive master list of agency points of contacts to be developed and promulgated by OPM (see attachment 3 for prescribed "Inter-Agency Clearance Verification Request" and attachment 4 for a draft "Master List of Agency Contacts"). A listing of agency points of contact is posted along with prescribed verification format to OPM's web portal site, <https://opmis.xsp.org>.
 - (c) **Required Action:** **Agencies will begin daily updates to OPM's Clearance Verification System (CVS) and to update existing entries by March 31, 2006.** This date is dependent upon the ability of affected agencies to develop and implement the necessary technical interfaces that will permit daily updates. An OPM directed working group is currently examining what barriers exist to all agencies using this system and will resolve those issues as they arise.
3. **Issue:** A permitted exception to reciprocity may occur when an individual is being considered for access to a program of a sensitivity level different from that of the existing program. This step only applies to SCI, SAP and Q programs and only when the new program has investigative and/or adjudicative criteria at the time the program is approved by the agency head or deputy that are higher than standards set forth in Executive Order 12968 (applies to State, Energy, Defense, DHS, CIA and DNI only – the only agencies authorized to establish SAPs). Reciprocity has proved most elusive when individuals (especially cleared contractors) cross over to different programs that entail access to TOP SECRET, SAP and/or SCI information. This is due, in part, to the significant discretion agency heads had been granted by Executive Order 12968 to establish "additional but not duplicative investigative or adjudicative criteria" for SAPs, to include SCI. While no standards exist regarding acceptable higher investigative or adjudicative criteria and the circumstances under which they are appropriate – the two most common are: i) a requirement for a polygraph examination, and ii) outright disqualification

based upon non-U.S. immediate family members (although the latter is the most frequently waived disqualifier).

- (a) **Required Action:** OPM is configuring CVS to reflect on a real-time basis those individuals who have undergone a polygraph (as the Intelligence Community's Scattered Castles database currently does) and agencies must begin inputting required data for all new and existing clearances on December 17, 2005.
 - (b) **Required Action:** For those agencies without access to Scattered Castles, or to verify polygraphs at agencies that don't post to Scattered Castles, OPM will provide in the aforementioned clearance verification request and master list of agency points of contact the means to manually verify via phone or fax whether an individual has undergone a polygraph examination. This information can be found on OPM's web portal (<https://opmis.xsp.org>).
 - (c) **Required Action:** **Agencies will update by March 31st, 2006 their records in OPM's Clearance Verification System to reflect those cleared individuals who have undergone a polygraph and/or, to the extent practical, have non-U.S. immediate family members.** (While reflecting non-U.S. immediate family members for new clearances should not prove difficult, it may be problematic for those agencies without the authority to grant SCI or SAP access to annotate existing records).
 - (d) **Required Action:** **While Executive Order 12968 allows agency heads to establish additional but not duplicative investigative or adjudicative requirements for SAPs, to include SCI, agencies will, in accordance with Executive Order 13381:**
 - **Limit such additional requirements to the polygraph examination and/or disqualifying individuals based upon non-U.S. immediate family; and**
 - **Ensure that programs desiring to utilize or continue to use additional requirements other than the above for the purpose of determining eligibility for access to classified information first obtain the approval of the Director of OMB in accordance with §3001(d)(3)(A), Title III, Public Law 108-548 by January 31, 2006 and as new programs are established thereafter.**
 - (e) **Required Action:** The Personnel Security Working Group of the Records Access and Information Security PCC will evaluate the need to formalize changes to existing policy documents that codifies the above by January 31, 2006.
4. **Issue:** Oftentimes, it is difficult to distinguish between employment suitability issues and security clearance trustworthy issues. Unique suitability issues serve as impediments to reciprocity. For example, a military veteran or a contractor employee with a current, final Secret clearance is not eligible for immediate Federal employment since the suitability investigation for Federal employment differs from the investigation for a Secret clearance.
- (a) **Required Action:** The Personnel Security Working Group of the Records Access and Information Security PCC will evaluate by February 28, 2006 the need for policy changes that ensure consistency between the basic investigative requirement to determine suitability for Federal employment and the basic investigative requirement for access to information classified Secret and below.

- (b) **Required Action:** As this is being developed, agencies must be cognizant that unique suitability issues such as requirements for psychological or medical evaluations as well as the unwillingness to accept certain mitigated issues (e.g. past drug usage of any vintage serving as a bar to employment as a DEA agent) will always contribute to the perception that reciprocity is not being honored. **Agencies must ensure that in such instances, the completion of an entirely new security questionnaire or the conduct of duplicative investigative checks does not occur. Rather, only additional, not duplicative, investigative and adjudicative procedures will be completed.**
5. **Issue:** Lack of reciprocity often arises when there is reluctance to be accountable for poor quality investigations and/or adjudications conducted by prior agencies or organizations. While reciprocity has proved elusive by fiat and in the absence of any accountability for performance, confidence among security practitioners in the quality of each other's work can be increased.
- (a) **Required Action:** Working with the Department of Defense, the Intelligence Community has developed standardized training for all adjudicators. This week-long course enhances the level of competence and understanding of adjudication fundamentals to include the principles of reciprocity by systematically presenting the Adjudicative Guidelines, providing practical hands-on case studies, and exposing students to a coherent way of thinking about adjudication. In this vein, the Reciprocity Working Group will identify by February 15, 2006 additional opportunities to provide such content to adjudicators Executive branch-wide through uniform, high quality training, along with opportunities for better communication with all security managers and adjudicators to ensure familiarity with and understanding of the "new way of doing business."
- (b) **Required Action:** An important way to foster mutual confidence is to provide mechanisms where personnel security practitioners can collaborate on issues of common interest. The intelligence community is convening a forum for such collaboration under the name "Common Adjudicative Procedures for the SCI Community" or CAPSC. This forum shall be expanded Executive branch-wide to include the non-SCI community and be assigned specific responsibilities to report to OMB.
6. **Issue:** Metrics are essential in order to measure progress.
- (a) **Required Action:** The aforementioned CAP Forum, with respect to any agency's adjudicative activity relating to the issuing of security clearances to include posting data to CVS, is assigned responsibility to: consider and make recommendations to OMB on complaints and suggestions; organize and oversee periodic on-site peer reviews; and provide quarterly progress reports to OMB.
- (b) **Required Action:** For industry, through the "MOU Associations," contractors shall report quarterly, on a voluntary basis, the total number of times their employees have completed a security questionnaire and of those, the number of times it appeared to the contractor to be in contravention of the "Checklist of Acceptable Exceptions to Reciprocity." These trend reports would be submitted through the Information Security Oversight Office.
- (c) **Required Action:** Additional metrics for measuring agencies' progress toward meeting the reciprocity standards will be developed within 60 days and provided to you.
- (d) **Required Action:** **Agencies will be expected to report to OMB by April 1, 2006, the status of their implementation of the new procedures relative to the reciprocity of**

access eligibility determinations, to include the updating of agency regulations, as appropriate. OMB will provide you with a format for that report.

- (e) **Required Action:** OMB will issue a report by May 1, 2006 which provides feedback to agencies on the progress made Executive branch-wide with respect to the reciprocity of access eligibility determinations.

Milestones

Task	Responsible Party	Due Date
1. Master List of Agency Contacts posted to OPM web portal	OPM	Complete
2. Procedures for verifying existing access eligibility determinations posted to OPM web portal	OPM	12/15/05
3. Procedures for joining collaboration forum for adjudicators posted to OPM web portal	OPM	12/15/05
4. Finalize format for industry trend reports	NARA	Complete
5. Initial organizing meeting of collaboration forum	DNI	12/15/05
6. Additional data fields essential for reciprocity available in CVS	OPM	12/17/05
7. Deadline for agencies wanting to continue criteria over and above polygraph and non-U.S. immediate family member disqualifier for existing programs to request specific approval from OMB	Agencies	1/31/06
8. Reciprocity Working Group to identify additional opportunities to present uniform, high quality training and to enhance communication	NARA	2/15/06
9. Reciprocity WG to identify additional metrics for measuring agencies progress toward meeting the reciprocity standards	NARA	2/15/06
10. PCC evaluation of need for additional policy changes	PCC	2/28/06
11. Initial peer review of agency adjudicative responsibilities	NARA	3/1/06
12. Initial agency implementation reports submitted to OMB	Agencies	4/1/06
13. Initial forum report to OMB	DNI	4/1/06
14. Initial trend report from industry groups	NARA	4/1/06
15. Initial OMB report on the state of reciprocity	OMB	5/1/06
16. CVS IOC which allows agencies to update entries daily	OPM	TBD
17. CVS FOC which requires agencies to update daily those data fields essential for reciprocity for existing and new entries	OPM	TBD

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, NACLIC, 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?			
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?*			
6. If applicable , does the individual not satisfy a requirement imposed by the new program that does not allow any non-U.S. immediate family, as approved by the agency head or deputy? *			
7. If applicable and if approved by OMB , other than for questions 5 and 6 above, does the individual not satisfy an investigative and/or adjudicative criterion that is additional to the standards set forth in E.O. 12968?*			

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>

* Under such circumstances, the completion of an entirely new security questionnaire is not authorized. Rather, only additional – not duplicative – investigative or adjudicative procedures will be completed.

CVS Reciprocity Data Elements

The following 19 items are the data elements required to be in the Clearance Verification System in order to support reciprocity. The remarks, keyed to the line numbers, explain what each element includes and, where necessary, detailed information about how to formulate it.

Identity

1. Name, last
2. Name, first
3. Name, middle
4. Name, suffix
5. SSN
6. DOB

Investigation

7. Investigation type
8. Investigation date
9. Polygraph type
10. Polygraph agency
11. Polygraph date

Clearance

12. Clearance Level
13. Special Access
14. Date of Eligibility
15. Interim clearance
16. Status
17. Adjudicative authority

Alerts

18. Non-US Immediate Family
19. PLEASE CALL

REMARKS

Entries are in ALL CAPS.

1. Last name. Convention: Reflect spacing in multi-word names (e.g., DE SILVA, not DESILVA), hyphens in hyphenated names (e.g., SCHMITT-WALTER, not SCHMITT WALTER or SCHMITTWALTER), and apostrophes in names with them (e.g., O'NEILL, not ONEILL). Ignore non-standard characters (e.g., GLUCK, not GLÜCK; GUINOT, not GUINÔT; NGO DINH, not NGÔ ĐÌNH). Treat ligatures as separate letters (e.g., FAERNISE, not FÆRNISE); reflect German ß as SS.

2. First name. Convention: as above. Use "(IO)" to indicate initial only [e.g., E. (IO)]. Include periods with initials.

3. Middle name. Convention: as above. Use "(IO)" to indicate initial only [e.g., E. (IO)]; use "(NMN)" to indicate no middle name. Include periods with initials. If a person has more than one

middle name, include only the first (e.g., reflect John Robert Thomas Duran’s middle name as ROBERT, not ROBERT THOMAS).

4. Suffix. JR., SR., II, III, IV, etc. Do not include honorifics (e.g., ESQ.), degrees (e.g., M.D.) or anything else not integral to the person’s name. If none, leave blank.

5. SSN. Use nine consecutive digits, without spaces or hyphens (e.g., 000000000, not 000-00-0000 or 000 00 0000).

6. DOB. Use the DD-MMM-YYYY convention: thus reflect July 4, 1976 as 04-JUL-1976.

7. Investigation type. List the most recently completed personnel security investigation, using standard designators, e.g., SSBI, SSBI-PR, NACL, ANACI, NACI, MBI.

8. Investigation date. Use the closing date appearing on the investigation, *not* the initiation date or date of adjudication. Use the DD-MMM-YYYY convention.

9. Polygraph type. This and the following two fields relate only to polygraphs administered as a part of security processing. Record only the most recent polygraph. Reflect the type as either CI (counterintelligence scope) or FS (full scope). If there is no polygraph, enter NONE.

10. Polygraph agency. Use the standard designator for the agency administering the polygraph (e.g., CIA, NRO, NSA). Use USAF for Air Force, USN for Navy, and USA for Army.

11. Polygraph date. Use the date of the examination as reflected in agency records.

12. Clearance level. Reflect the highest level of clearance: Use CONF for Confidential, SEC for Secret, and TS for Top Secret. Use NONE if no clearance determination has been made or if the person has been determined ineligible (denied or revoked). For DOE access authorizations, use L or Q.

13. Special Access. Reflect whether the person has been determined eligible for either Sensitive Compartmented Information, other Special Access Programs, or both. Use SCI, SAP, and SAPSCI. If no special access eligibility has been determined, enter NONE.

Note: Items 12 and 13, when taken together, indicate the type of adjudication the person has undergone. Some examples:

<i>Clnc Level</i>	<i>Sp Acc</i>	<i>Meaning</i>
TS	NONE	Favorable adjudication for TS, no SCI or SAP determination
TS	SCI	Favorable adjudication for Top Secret with eligibility for SCI
SEC	NONE	Favorable adjudication for Secret, no SAP determination
SEC	SAP	Favorable adjudication for Secret and for SAPs at the Secret (but not Top Secret) level
TS	SAPSCI	Favorable adjudication for Top Secret with eligibility for both Top Secret SAPs and SCI

14. Date of eligibility. Date of the most recent favorable adjudication. Use the DD-MMM-YYYY convention.

15. Interim clearance. Indicate YES if the clearance level reflected in the record is based on an open investigation. Otherwise enter NO.

16. Status. Use ACTIVE (meaning the person currently occupies a position requiring some level of classified access), SUSP (meaning the person has been suspended from access but not debriefed), or DEBR (meaning the person is currently debriefed from all classified access). DEBR is without respect for reason.

17. Adjudicative authority. Standard designator of the agency granting the clearance eligibility.

18. Non-US immediate family. Enter YES if any of the person's living immediate family members (father, mother, brother, sister, spouse, son, daughter, or cohabitant) is not a US citizen. Each of these terms includes all its variants; e.g., "sister" includes sister by blood, sister by adoption, half-sister, stepsister, and foster sister. If all immediate family members are US citizens, enter NONE.

19. PLEASE CALL. Use PLEASE CALL to alert system users only if one of the following applies:

- ◆ waivers (access eligibility granted or continued despite the presence of substantial issue information that would normally preclude access);
- ◆ conditions (access eligibility granted or continued with the proviso that one or more additional measures will be required, such as additional security monitoring, restrictions on access, and restrictions on an individual's handling of classified information);
- ◆ deviations (access eligibility granted or continued despite either a significant gap in coverage—meaning complete lack of coverage of a period of six months or more within the most recent five years investigated—or a significant deficiency in the scope in the investigation, such as the absence of all employment checks);¹
- ◆ suspensions of access;
- ◆ revocations of access;
- ◆ denials of access; and
- ◆ ongoing investigations that could affect the person's continued eligibility for access.

¹ Do not use PLEASE CALL to flag cases with out-of-date investigations unless one of the other reasons in this list applies.

Some Sample Records

1. TS clearance, no SAP or SCI

Name Last BRAUNBOX	Name First THEODORE	Name Middle MICHAEL	Name Suffix JR.	SSN 000000000	DOB 03-MAY-1902
Inv Type SSBI-PR	Inv Date 05-JUN-2002	Poly Type NONE	Poly Agency	Poly Date	
Clnc Level TS	Spec Access NONE	Date of Elig 06-AUG-2002	Interim Clnc NO	Status ACTIVE	Adj Auth JUSTICE
Non-US Fam NONE					

2. Secret clearance, foreign relatives

Name Last LAUFKOETTER	Name First MARY	Name Middle (NMN)	Name Suffix	SSN 000000000	DOB 06-DEC-1983
Inv Type NACLC	Inv Date 30-APR-2005	Poly Type NONE	Poly Agency	Poly Date	
Clnc Level SEC	Spec Access SAP	Date of Elig 06-MAY-2005	Interim Clnc NO	Status ACTIVE	Adj Auth USAF
Non-US Fam YES					

3. TS clearance, SCI eligibility with a condition applied, polygraph

Name Last QWINE	Name First FRANK	Name Middle R. (IO)	Name Suffix	SSN 000000000	DOB 17-FEB-1950
Inv Type SSBI	Inv Date 26-MAY-2000	Poly Type FS	Poly Agency CIA	Poly Date 13-JUN-2001	
Clnc Level TS	Spec Access SCI	Date of Elig 10-NOV-2003	Interim Clnc NO	Status ACTIVE	Adj Auth CIA
Non-US Fam NONE	PLEASE CALL				

4. Favorably adjudicated for Secret, not currently in access

Name Last ASQUE	Name First SANDRA	Name Middle SARAH	Name Suffix	SSN 000000000	DOB 09-NOV-1961
Inv Type ANACI	Inv Date 05-MAR-2004	Poly Type NONE	Poly Agency	Poly Date	
Clnc Level SEC	Spec Access NONE	Date of Elig 11-APR-2004	Interim Clnc NO	Status DEBR	Adj Auth TREASURY
Non-US Fam NONE					

5. Temporary access eligibility

Name Last HEAP	Name First URIAH	Name Middle DICKENS	Name Suffix III	SSN 000000000	DOB 22-AUG-1970
Inv Type NONE	Inv Date	Poly Type NONE	Poly Agency	Poly Date	
Cln Level SEC	Spec Access NONE	Date of Elig 6-AUG-2002	Interim Cln YES	Status ACTIVE	Adj Auth COMMERCE
Non-US Fam NONE					

5. Access revoked

Name Last MALAHIDE	Name First MARY	Name Middle BARBARA	Name Suffix	SSN 000000000	DOB 05-MAY-1977
Inv Type SSBI	Inv Date 17-MAY-2002	Poly Type CS	Poly Agency USAF	Poly Date 03-NOV-2004	
Cln Level NONE	Spec Access NONE	Date of Elig	Interim Cln NO	Status DEBR	Adj Auth USAF
Non-US Fam NONE	PLEASE CALL				

6. Access suspended

Name Last BOSKNECHT	Name First IAGO	Name Middle RONALD	Name Suffix SR.	SSN 000000000	DOB 30-JUN-1935
Inv Type SSBI	Inv Date 17-MAY-2002	Poly Type NONE	Poly Agency	Poly Date	
Cln Level TS	Spec Access SCI	Date of Elig 27-MAY-2002	Interim Cln NO	Status SUSP	Adj Auth USAF
Non-US Fam NONE	PLEASE CALL				

Inter-Agency Clearance Verification Request

The U.S. Government agency indicated below is requesting that you provide them with specific data pertaining to security clearance information your agency might maintain on the subject whose identifying information is provided hereon. This request is being made because a search of appropriate databases failed to disclose pertinent information.

SUBJECT NAME: _____
Last First Middle Suffix
SSN: _____ DOB: _____

CLEARANCE (C/S/TS): _____ GRANT DATE: _____

IS THIS CLEARANCE ACTIVE? YES _____ NO _____

IF NO, WAS THIS CLEARANCE: SUSPENDED _____ REVOKED _____
ADMINISTRATIVELY WITHDRAWN _____ DENIED _____
PROVIDE DATE OF ACTION FOR ANY OF THE ABOVE: _____

IS THIS AN INTERIM OR TEMPORARY CLEARANCE? YES _____ NO _____

WHAT AGENCY ADJUDICATED THIS CLEARANCE? _____

INVESTIGATIVE BASIS:

TYPE OF INVESTIGATION: _____ DATE INVESTIGATION CLOSED: _____

WHAT AGENCY CONDUCTED THE INVESTIGATION? _____

(FOR ACCESS TO HIGHLY SENSITIVE PROGRAMS ONLY)

COMPLETE THE BELOW ITEMS ONLY IF CHECKED:

_____ DOES THIS CLEARANCE CARRY ANY WAIVERS, DEVIATIONS OR CONDITIONS?
YES _____ NO _____

_____ WAS A POLYGRAPH EXAMINATION CONDUCTED? YES _____ NO _____

IF YES, INDICATE TYPE: _____ DATE: _____ AGENCY: _____

_____ DOES THE SUBJECT HAVE ANY NON-U.S. FAMILY MEMBERS?
YES _____ NO _____

PLEASE COMPLETE THIS FORM AND RETURN IT AS SOON AS POSSIBLE TO:

AGENCY NAME: _____

CONTACT PERSON: _____

FAX: _____ PHONE: _____



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

DEPUTY DIRECTOR
FOR MANAGEMENT

July 17, 2006

M-06-21

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, NACLC, 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.

**INTELLIGENCE REFORM AND TERRORISM PREVENTION
ACT OF 2004 (Public Law No: 108-458)**

TITLE III—SECURITY CLEARANCES

SEC. 3001. SECURITY CLEARANCES.

(a) DEFINITIONS.—In this section:

(1) The term “agency” means—

(A) an executive agency (as that term is defined in section 105 of title 5, United States Code);

(B) a military department (as that term is defined in section 102 of title 5, United States Code); and

(C) an element of the intelligence community.

(2) The term “authorized investigative agency” means an agency designated by the head of the agency selected pursuant to subsection (b) to conduct a counterintelligence investigation or investigation of persons who are proposed for access to classified information to ascertain whether such persons satisfy the criteria for obtaining and retaining access to such information.

(3) The term “authorized adjudicative agency” means an agency authorized by law, regulation, or direction of the Director of National Intelligence to determine eligibility for access to classified information in accordance with Executive Order 12968.

(4) The term “highly sensitive program” means—

(A) a government program designated as a Special Access Program (as that term is defined in section 4.1(h) of Executive Order 12958 or any successor Executive order);

or

(B) a government program that applies restrictions required for—

(i) restricted data (as that term is defined in section 11 y. of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)); or

(ii) other information commonly referred to as “sensitive compartmented information”.

(5) The term “current investigation file” means, with respect to a security clearance, a file on an investigation or adjudication that has been conducted during—

(A) the 5-year period beginning on the date the security clearance was granted, in the case of a Top Secret Clearance, or the date access was granted to a highly sensitive program;

(B) the 10-year period beginning on the date the security clearance was granted in the case of a Secret Clearance;

And

(C) the 15-year period beginning on the date the security clearance was granted in the case of a Confidential Clearance.

(6) The term “personnel security investigation” means any investigation required for the purpose of determining the eligibility of any military, civilian, or government contractor personnel to access classified information.

(7) The term “periodic reinvestigations” means investigations conducted for the purpose of updating a previously completed background investigation—

(A) every 5 years in the case of a top secret clearance or access to a highly sensitive program;

(B) every 10 years in the case of a secret clearance;

Or

(C) every 15 years in the case of a Confidential Clearance.

(8) The term “appropriate committees of Congress” means—

(A) the Permanent Select Committee on Intelligence and the Committees on Armed Services, Homeland Security, Government Reform, and the Judiciary of the House of Representatives; and

(B) the Select Committee on Intelligence and the Committees on Armed Services, Homeland Security and Governmental Affairs, and the Judiciary of the Senate.

(b) SELECTION OF ENTITY.—Not later than 90 days after the date of the enactment of this Act, the President shall select a single department, agency, or element of the executive branch to be responsible for—

(1) directing day-to-day oversight of investigations and adjudications for personnel security clearances, including for highly sensitive programs, throughout the United States Government;

(2) developing and implementing uniform and consistent policies and procedures to ensure the effective, efficient, and timely completion of security clearances and determinations for access to highly sensitive programs, including the standardization of security questionnaires, financial disclosure requirements for security clearance applicants, and polygraph policies and procedures;

(3) serving as the final authority to designate an authorized investigative agency or authorized adjudicative agency;

(4) ensuring reciprocal recognition of access to classified information among the agencies of the United States Government, including acting as the final authority to arbitrate and resolve disputes involving the reciprocity of security clearances and access to highly sensitive programs pursuant to subsection (d);

(5) ensuring, to the maximum extent practicable, that sufficient resources are available in each agency to achieve clearance and investigative program goals; and

(6) reviewing and coordinating the development of tools and techniques for enhancing the conduct of investigations and granting of clearances.

(c) PERFORMANCE OF SECURITY CLEARANCE INVESTIGATIONS.—

(1) Notwithstanding any other provision of law, not later than 180 days after the date of the enactment of this Act, the President shall, in consultation with the head of the entity selected pursuant to subsection (b), select a single agency of the executive branch to conduct, to the maximum extent practicable, security clearance investigations of employees and contractor personnel of the United States Government who require access to classified information and to provide and maintain all security clearances of such employees and contractor personnel. The head of the entity selected pursuant to subsection (b) may designate other agencies to conduct such investigations if the head of the entity selected pursuant to subsection (b) considers it appropriate for national security and efficiency purposes.

(2) The agency selected under paragraph (1) shall—

(A) take all necessary actions to carry out the requirements of this section, including entering into a memorandum of understanding with any agency carrying out responsibilities relating to security clearances or security clearance investigations before the date of the enactment of this Act;

(B) as soon as practicable, integrate reporting of security clearance applications, security clearance investigations, and determinations of eligibility for security clearances, with the database required by subsection (e); and

(C) ensure that security clearance investigations are conducted in accordance with uniform standards and requirements established under subsection (b), including uniform security questionnaires and financial disclosure requirements.

(d) RECIPROCITY OF SECURITY CLEARANCE AND ACCESS DETERMINATIONS.

—(1) All security clearance background investigations and determinations completed by an authorized investigative agency or authorized adjudicative agency shall be accepted by all agencies.

(2) All security clearance background investigations initiated by an authorized investigative agency shall be transferable to any other authorized investigative agency.

(3)(A) An authorized investigative agency or authorized adjudicative agency may not establish additional investigative or adjudicative requirements (other than requirements for the conduct of a polygraph examination) that exceed requirements specified in Executive Orders establishing security requirements for access to classified information without the approval of the head of the entity selected pursuant to subsection (b).

(B) Notwithstanding subparagraph (A), the head of the entity selected pursuant to subsection (b) may establish such additional requirements as the head of such entity considers necessary for national security purposes.

(4) An authorized investigative agency or authorized adjudicative agency may not conduct an investigation for purposes of determining whether to grant a security clearance to an individual where a current investigation or clearance of equal level already exists or has been granted by another authorized adjudicative agency.

(5) The head of the entity selected pursuant to subsection (b) may disallow the reciprocal recognition of an individual security clearance by an agency under this section on a case-by-case basis if the head of the entity selected pursuant to subsection (b) determines that such action is necessary for national security purposes.

(6) The head of the entity selected pursuant to subsection (b) shall establish a review procedure by which agencies can seek review of actions required under this section.

(e) DATABASE ON SECURITY CLEARANCES.—(1) Not later than 12 months after the date of the enactment of this Act, the Director of the Office of Personnel Management shall, in cooperation with the heads of the entities selected pursuant to subsections (b) and (c), establish and commence operating and maintaining an integrated, secure, database into which appropriate data relevant to the granting, denial, or revocation of a security clearance or access pertaining to military, civilian, or government contractor personnel shall be entered from all authorized investigative and adjudicative agencies.

(2) The database under this subsection shall function to integrate information from existing Federal clearance tracking systems from other authorized investigative and adjudicative agencies into a single consolidated database.

(3) Each authorized investigative or adjudicative agency shall check the database under this subsection to determine whether an individual the agency has identified as requiring a security clearance has already been granted or denied a security clearance, or has had a security clearance revoked, by any other authorized investigative or adjudicative agency.

(4) The head of the entity selected pursuant to subsection (b) shall evaluate the extent to which an agency is submitting information to, and requesting information from, the database under this subsection as part of a determination of whether to certify the agency as an authorized investigative agency or authorized adjudicative agency.

(5) The head of the entity selected pursuant to subsection (b) may authorize an agency to withhold information about certain individuals from the database under this subsection if the head of the entity considers it necessary for national security purposes.

(f) EVALUATION OF USE OF AVAILABLE TECHNOLOGY IN CLEARANCE INVESTIGATIONS AND ADJUDICATIONS.—

(1) The head of the entity selected pursuant to subsection (b) shall evaluate the use of available information technology and databases to expedite investigative and adjudicative processes for all and to verify standard information submitted as part of an application for a security clearance.

(2) The evaluation shall assess the application of the technologies described in paragraph (1) for—

(A) granting interim clearances to applicants at the secret, top secret, and special access program levels before the completion of the appropriate full investigation;

(B) expediting investigations and adjudications of security clearances, including verification of information submitted by the applicant;

(C) ongoing verification of suitability of personnel with security clearances in effect for continued access to classified information;

(D) use of such technologies to augment periodic reinvestigations;

(E) assessing the impact of the use of such technologies on the rights of applicants to verify, correct, or challenge information obtained through such technologies; and

(F) such other purposes as the head of the entity selected pursuant to subsection (b) considers appropriate.

(3) An individual subject to verification utilizing the technology described in paragraph (1) shall be notified of such verification, shall provide consent to such use, and shall have access to data being verified in order to correct errors or challenge information the individual believes is incorrect.

(4) Not later than one year after the date of the enactment of this Act, the head of the entity selected pursuant to subsection (b) shall submit to the President and the appropriate committees of Congress a report on the results of the evaluation, including recommendations on the use of technologies described in paragraph (1).

(g) REDUCTION IN LENGTH OF PERSONNEL SECURITY CLEARANCE PROCESS.—

(1) The head of the entity selected pursuant to subsection (b) shall, within 90 days of selection under that subsection, develop, in consultation with the appropriate committees of Congress and each authorized adjudicative agency, a plan to reduce the length of the personnel security clearance process.

(2)(A) To the extent practical the plan under paragraph (1) shall require that each authorized adjudicative agency make a determination 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 for a security clearance by an authorized investigative agency. Such 60-day average period shall include—

(i) a period of not longer than 40 days to complete the investigative phase of the clearance review; and

(ii) a period of not longer than 20 days to complete the adjudicative phase of the clearance review.

(B) Determinations on clearances not made within 60 days shall be made without delay.

(3)(A) The plan under paragraph (1) shall take effect 5 years after the date of the enactment of this Act.

(B) During the period beginning on a date not later than 2 years after the date after the enactment of this Act and ending on the date on which the plan under paragraph (1) takes effect, each authorized adjudicative agency shall make a determination on at least 80 percent of all applications for a personnel security clearance pursuant to this section within an average of 120 days after the date of receipt of the application for a security clearance by an authorized investigative agency. Such 120-day average period shall include—

(i) a period of not longer than 90 days to complete the investigative phase of the clearance review; and

(ii) a period of not longer than 30 days to complete the adjudicative phase of the clearance review.

(h) REPORTS.—(1) Not later than February 15, 2006, and annually thereafter through 2011, the head of the entity selected pursuant to subsection (b) shall submit to the appropriate committees of Congress a report on the progress made during the preceding year toward meeting the requirements of this section.

(2) Each report shall include, for the period covered by such report—

(A) the periods of time required by the authorized investigative agencies and authorized adjudicative agencies for conducting investigations, adjudicating cases, and granting clearances, from date of submission to ultimate disposition and notification to the subject and the subject's employer;

(B) a discussion of any impediments to the smooth and timely functioning of the requirements of this section; and

(C) such other information or recommendations as the head of the entity selected pursuant to subsection (b) considers appropriate.

(i) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated such sums as may be necessary for fiscal year 2005 and each fiscal year thereafter for the implementation, maintenance, and operation of the database required by subsection (e).