AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

Union Calendar No. 591

110TH CONGRESS, 2d Session | HOUSE OF REPRESENTATIVES | REPORT 110–916

SECURITY CLEARANCE REFORM—UPGRADING THE GATEWAY TO THE NATIONAL SECURITY COMMUNITY

SUBMITTED BY MR. REYES, CHAIRMAN, PERMANENT SELECT COMMITTEE ON INTELLIGENCE

NOVEMBER 20, 2008.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

U.S. GOVERNMENT PRINTING OFFICE

79–006 WASHINGTON : 2008

SUBCOMMITTEE ON INTELLIGENCE COMMUNITY MANAGEMENT

ANNA G. ESHOO, California, *Chair*

RUSH HOLT, New Jersey
C.A. "DUTCH" RUPPERSBERGER, Maryland
MIKE THOMPSON, California
PATRICK J. MURPHY, Pennsylvania
SILVESTRE REYES, Texas, *Chairman, ex officio*

DARRELL ISSA, California, *Ranking Member*
MAC THORNBERRY, Texas
TODD TIAHRT, Kansas
PETER HOEKSTRA, Michigan, *ex officio*

MIEKE EOYANG, *Professional Staff Member*
DIANE LA VOY, *Professional Staff Member*
JOSH RESNICK, *Research Assistant*
JAMAL WARE, *Professional Staff Member*

CONTENTS

	Page
Methodology	1
Summary	1
Security Clearances in the U.S. Government	4
Security Clearances in the Intelligence Community	6
Long-Standing Congressional Concerns	7
Views of Industry	9
Requirements of the Intelligence Reform and Terrorism Prevention Act of 2004	11
Implementation Authorities and Plans	13
Assessing Performance Against IRTPA Requirements	14
Current Reforms: Issues for Oversight	20

Union Calendar No. 591

110TH CONGRESS, 2d Session } HOUSE OF REPRESENTATIVES { REPORT 110–916

SECURITY CLEARANCE REFORM—UPGRADING THE GATEWAY TO THE NATIONAL SECURITY COMMUNITY

NOVEMBER 20, 2008.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. REYES, from the Permanent Select Committee on Intelligence, submitted the following

R E P O R T

METHODOLOGY

This report was prepared on the basis of transcripts and statements for the record used in subcommittee hearings held in open session, reports by the Government Accountability Office and other publicly available materials. No classified material was used in the preparation of this report.

SUMMARY

Security clearances, which are determinations that a person is eligible for access to classified information, enable millions of Americans to serve our country in the arenas of national security, homeland security, and foreign policy. The number of federal government employees and contractors requiring clearances has expanded in recent decades, especially in the aftermath of the September 11, 2001, terrorist attacks. As a result, backlogs developed and the length of time for processing security clearances grew. In turn, greater awareness of the need to share information and promote collaboration across government agencies drew attention to the cumbersome and outdated nature of the process for granting security clearances and for ensuring that clearances granted by one agency permit access to the others.

Under Title III of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), the Office of Personnel Management (OPM) assumed responsibility for the majority of security clearance investigations, previously performed by the Department of Defense (DOD); and the Office of Management and Budget (OMB) became

the entity responsible for security clearance policy and procedures across the U.S. Government.

Throughout the 110th Congress, the House Permanent Select Committee on Intelligence's Subcommittee on Intelligence Community Management (the Subcommittee or ICM) has monitored the implementation of reforms of the security clearance process embodied in IRTPA. It has focused its attention on the Intelligence Community, whose personnel hold approximately 10 percent of the total number of security clearances. The Subcommittee's oversight has built on over 25 years of congressional concerns about security clearances, including numerous studies by Congress's Government Accountability Office (GAO).

A key feature of Title III of IRTPA, which aims to bring greater efficiency, speed and interagency reciprocity to the clearance process, is the centralization of responsibility. The following is a summary of how the requirements of Title III have been met.

Centralization of policy oversight and management

Assessment: Actions have been taken, but progress has been mixed

In 2005, President George W. Bush selected OMB to be responsible for policy and oversight of the security clearance process. OMB, in turn, delegated to OPM responsibility for security clearance investigations, to "maintain security clearances, and to integrate security clearance information across all agencies." [1]

In April 2008, the Administration announced a change to that structure, designating a collaborative effort consisting of representatives of DOD, OMB, the Office of the Director of National Intelligence (ODNI), and OPM, called the Joint Security and Suitability Reform Team. The structure, formalized by executive order in June 2008, creates a Performance Accountability Council to achieve the goals of security clearance reform. This Council, to be chaired by OMB's Deputy Director for Management, includes the DNI as the "Security Executive Agent" responsible for security clearances government-wide; and affirms the Director of OPM as responsible for the federal government's workforce.

While both the old and new structures seem to meet the law's requirements, the first structure did not demonstrate concrete results towards several of the IRTPA's requirements. While it is too early to evaluate the success of the new structure, it appears that steps have been taken to improve the system.

Single agency for investigations

Assessment: The requirement has been partially met

This provision, which requires that a single agency shall, "to the maximum extent practicable," be responsible for conducting security clearance investigations, has been partially implemented. The statute also requires this entity to integrate security clearance applications, investigations, and determinations into a database, and ensure security clearance investigations are conducted under uniform standards and requirements.

[1] IRTPA. § 3001(c).

For practical purposes, OPM conducts most security clearance investigations in the government, but few of the investigations for the Intelligence Community. OPM has not met the requirements regarding databases. The DNI, as the new Security Executive Agent, is undertaking a review of the investigative standards and adjudicative guidelines.

Interagency reciprocity

Assessment: The standard set forth by IRTPA has not been met

Although the law requires that "all security clearance background investigations and determinations . . . shall be accepted by all agencies," policy interpretations by OPM and the DNI, and language in various executive orders and Administration reports, have been inconsistent. Most problematic is that the Administration still does not measure progress toward full reciprocity. In practice, security clearance adjudications are not fully accepted reciprocally across the U.S. Government, and anecdotal information shows that even among the elements of the Intelligence Community there are impediments and sometimes lengthy delays in granting clearances to employees detailed from one agency to another.

Integrated, secure database

Assessment: The requirement has not been met

The law calls for a database "into which appropriate data . . . shall be entered from all [emphasis added] authorized investigative and adjudicative agencies."[2]

OPM and DOD databases have been linked, but they do not include data about clearances that are not investigated by OPM, such as the Department of Homeland Security and the Department of State. Neither do they include Intelligence Community data, which is held separately.

In practice, neither the OPM nor the Intelligence Community has enabled the Administration to respond to questions from the Subcommittee regarding the number of security clearances that are held or how the number has grown.

Evaluate the use of available technologies

Assessment: This requirement has been met

The law requires that, by December 2005, OMB submit a report to the President and Congress on the results of an evaluation of the use of available information technology to expedite clearance processes. No such report was produced.

However, the Joint Reform Team did oversee a series of demonstration projects to evaluate new information technology (IT) services for the clearance process. The demonstrations included evaluations of paperless applications, fingerprint scanners, computerized interviews, automated record checks, automated reinvestigations, and automated adjudications. An integrated, end-to-end pilot is supposed to be conducted in coming months. These efforts were reported to Congress in 2008.

[2] IRTPA. § 3001(e).

Reduce the length of the clearance process

Assessment: The interim standards for timeliness that were to have been met by December 2006 were met on average across all the agencies processing security clearances

IRTPA set interim standards for timeliness which required that determinations be reached on at least 80 percent of all applications within an average of 120 days after receiving the application. The Administration reports that the interim standard was met in the first quarter of FY 2007. The data provided suggest that this standard was not met by each agency, and its presentation creates the best possible picture from what is, upon closer inspection, a mixed record. Nevertheless, the improvement in timeliness achieved by late 2006 was a remarkable achievement, particularly by OPM, which had inherited large backlogs of clearances to be processed when it assumed responsibility for the vast majority of the government's security clearances in 2005.

IRTPA standards require that by December 2009, 90% of all applications shall be processed within an average of 60 days. This continues to pose a significant challenge for almost all agencies.

The standards for timeliness set forth in IRTPA aggregate Top Secret (TS) level clearances with those at the Secret (S) or Confidential (C) level. More meaningful measures of progress would consider timeliness of the TS clearances separately.

Reporting

Assessment: The Administration has met the requirements for annual reports required by IRTPA's Section 3001(h)

The Administration has missed many of the deadlines set in IRTPA, but has met the requirement or made progress towards the goals since the deadline. Although progress in security clearance reform has been slow, the Subcommittee remains committed to ensuring that the security clearance system fully accomplishes the mission set forth by the IRTPA. The Subcommittee intends to consider legislation early in the 111th Congress that would spur security clearance reform by requiring agencies to report to Congress on key metrics of the security clearance process.

SECURITY CLEARANCES IN THE U.S. GOVERNMENT

A security clearance is a determination that a person is eligible for access to classified information. For millions of Americans, at least 2.5 million of whom are military service members, DOD civilian employees, legislative personnel or industry personnel working for DOD and most of the other federal agencies,[3] security clearances are the gateway to national service and employment in the arenas of national security, homeland security, and foreign policy.

National security information is classified according to its level of sensitivity, which is determined by the amount of national security damage that its disclosure might cause. Determinations of ac-

[3] This estimate excludes personnel in the Intelligence Community, Department of State, and the Federal Bureau of Investigation. U.S. Government Accountability Office (GAO). Testimony Before the Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Committee on Homeland Security and Governmental Affairs, U.S. Senate "PERSONNEL CLEARANCES: Key Factors for Reforming the Security Clearance Process." GAO–08–776T. May 22, 2008.

cess to classified information, or security clearances, are granted according to the same three levels: Confidential (C), Secret (S), and Top Secret (TS). Access to "sensitive compartmented information" (SCI) is provided as a way of managing certain national security programs in the Intelligence Community, while the designation "Special Access Program" (SAP) is used in the DOD.

The security clearance process consists of three stages: application, investigation, and adjudication. In most cases, the first stage consists of completing an application form known as an SF–86. Stage two, the investigation, is currently done by sending investigators to the field to interview neighbors, co-workers, and others. Since 2005, OPM has conducted investigations for DOD and all agencies except those within the Intelligence Community, the Department of Homeland Security and Department of State. These entities conduct their own investigations. Stage three, adjudication, occurs when the agency reviews the results of the investigation to make a determination of fitness for a security clearance. The clearance process also includes reinvestigations every five years for persons holding TS and TS/SCI clearances, every 10 years for Secret level clearances, and every 15 years for Confidential clearances. Longer and more detailed investigations are required for access to the TS and TS/SCI level than for the Secret and Confidential level.

Determinations of suitability for employment are distinct from the determinations granting access to classified information and facilities. Suitability determinations consider whether an individual's character and conduct may have an impact on the integrity or efficiency of the service he or she would provide as an employee. Security clearance determinations consider factors that may make the person a risk to national security.

The number of positions requiring security clearances throughout the federal government and the contracting community is over two and a half million, and appears to have grown substantially in the years since the attacks of September 11, 2001. Reasons cited for the increase include the growth in defense and homeland security jobs; a decade-long trend toward privatizing federal jobs; and the increasingly sensitive technology that military personnel, government employees and contractors come into contact with through their jobs. More and more, requests for clearances are for TS level rather than Secret. For example, for DOD industry personnel in 1995, 17% of the requests were for the TS level, while in 2003, 27% were for TS clearances.[4] The number of security clearances had also grown substantially during the decades before 9/11, although it is believed to have decreased to some extent in the 1980s and early 1990s as a result of efforts to limit government exposure to espionage.

Unfortunately, comprehensive information about the number of clearances being processed, or currently held, across the U.S. Government is not available. Little historical data is available that would permit one to track changes over time.[5] This challenge is indicative of some of the problems to be addressed in reforming the security clearance process.

---

[4] GAO. Testimony before the Subcommittee on Intelligence Community Management, Permanent Select Committee on Intelligence, House of Representatives. "Personnel Clearances: Key Factors for Reforming the Security Clearance Process. GAO–08–352T. February 27, 2008.

[5] Responses to HPSCI staff inquiries from OMB, OPM, and ODNI.

Processing large numbers of security clearances and job-related suitability clearances, as well as keeping up with periodic reinvestigations, constitutes a huge management challenge. For example, as of January 2007, the federal government was processing approximately 1.9 million requests for background investigations annually for security clearances or for eligibility for employment or to fulfill agencies' other requirements.[6] The DOD, whose uniformed, civilian, and industry personnel hold most of the security clearances, has in recent years been faulted by Congress for not producing accurate projections of the number of clearances that it requires or reliable budget predictions for the processing of those clearances.[7]

SECURITY CLEARANCES IN THE INTELLIGENCE COMMUNITY

Approximately one-tenth of the security clearances in the federal government are provided by the Intelligence Community, consisting of sixteen agencies ranging widely in size and function. The clearances are held by both civilian and contract personnel.

The situation with regard to security clearances in the Intelligence Community is distinctive in several ways. First, for employees or contractors working in the Intelligence Community, a security clearance is essential to employment because their jobs require access to classified material and to intelligence facilities.[8] Therefore, the security clearance performs much of the role that a suitability clearance plays in other parts of the government.

Second, a high percentage of the clearances for intelligence personnel are at the TS or TS/SCI level[9], whereas in other parts of the government many of the clearances are at the Secret or Confidential level. Investigations for the TS level require more steps and more time than those conducted at the Secret or Confidential level.

Third, the widespread use by the Intelligence Community of classified information may heighten awareness of the need to protect sources and methods. This has resulted in each of the intelligence agencies developing its own standards for investigations and adjudications of security clearances.[10] This situation has not changed since the enactment of IRTPA, which required that a single agency in the federal government conduct all the investigations "to the maximum extent practicable," and that there be one single entity to ensure "uniform and consistent policies and procedures" for all security clearance adjudications.

Fourth, congressional oversight of security clearances in the Intelligence Community has not been as intense or public as has oversight of DOD clearances. Until 2008, when the Subcommittee

---

[6] Report of the Security Clearance Oversight Group Consistent with Title III of the Intelligence Reform and Terrorism Prevention Act of 2004, February 2007, transmitted by OMB.

[7] For example, GAO Testimony before the Subcommittee on Intelligence Community Management, Permanent Select Committee on Intelligence, House of Representatives. "Personnel Clearances: Key Factors for Reforming the Security Clearance Process. GAO–08–352T. February 27, 2008.

[8] There are a few exceptions, including work at CIA's Open Source Center.

[9] Data maintained by ODNI pertains only to personnel cleared to the TS/SCI level; ODNI was not able to tell the Committee what proportion of the security clearances in the IC were at that level. July 28, 2008, e-mail response from ODNI Kathleen Butler of Legislative Affairs to Diane La Voy.

[10] An exception is that since 2005, reinvestigations of security clearances held by DIA and NSA personnel are conducted by OPM, the entity selected by the President to conduct the investigations "to the maximum extent practicable."

requested assistance from GAO, Congress had not requested that GAO study security clearances across the Intelligence Community.

LONG-STANDING CONGRESSIONAL CONCERNS

Reports by GAO show that Congress has had concerns about the security clearance process for over twenty-five years. The principal concerns in these reports, which have dealt primarily with DOD, have varied over time.

Excessive number of clearances. A number of well-publicized espionage cases in the mid-1980s spurred congressional interest in limiting the number cleared individuals. One of these cases was the John A. Walker, Jr. espionage case in 1985, in which the former U.S. Navy communications specialist was accused of running a spy ring that was passing classified information to the U.S.S.R.

In response, the Permanent Subcommittee on Investigations of the Senate Committee on Governmental Affairs held a week-long hearing on federal government security clearance programs.[11] During the hearing, that subcommittee expressed its concern that the abundance of clearances made the protection of state secrets too difficult and recommended that the number of cleared individuals should be kept to a minimum. In June 1985, the Navy announced that in response to concerns about vulnerability to espionage it would reduce cleared personnel by 50 percent.[12] GAO confirmed that during the next two years, the number of employees and contractors holding DOD clearances fell by about 40 percent.[13]

In recent years, Congress has been concerned less about limiting the overall number of clearances and more concerned about how well the executive branch, particularly DOD, estimates the number of clearances it will need and then manages the cost and workload of processing them all.

Delays, backlogs. While congressional attention to security clearances diminished in the 1990s, the topic became a focus of concern in the wake of the terrorist attacks of September 11, 2001. Recognizing the Intelligence Community's urgent need for analysts with foreign language expertise and the increasing demand for cleared personnel for homeland security jobs, both Congress and the executive branch turned their attention to the need to speed up the security clearance process, which by FY 2004 was taking an average of 392 days for a TS clearance.[14]

A 2004 report by GAO, for example, estimated that DOD had a backlog of 270,000 investigations and 90,000 adjudications.[15] In particular, clearances for industry personnel were a growing problem. GAO reported that in FY 2003 it took an average of 375 days to process clearances of all levels needed by contractors.[16] A 2006 GAO study, which looked at 2,259 cases of defense industry per-

---

[11] Hearing #99–166. April 16–25, 1985.

[12] Halloran, Richard. Navy Orders Cut of 50% in Access to Security Data. The New York Times. June 12, 1985.

[13] GAO. "DOD Clearance Reduction and Related Issues." NSIAD–87–170BR. September 18, 1987.

[14] Report of the Security Clearance Oversight Group Consistent with Title III of the Intelligence Reform and Terrorism Prevention Act of 2004, February 2007, page 3.

[15] GAO. "DOD Personnel Clearances: Additional Steps Can be Taken to Reduce Backlogs and Delays in Determining Security Clearance Eligibility for Industry Personnel." GAO–04–632. May 26, 2004.

[16] Ibid.

sonnel, found that TS clearances for defense industry employees took 446 days, on average.[17]

Congress was concerned about the impacts caused by long delays in processing security clearances. Long delays discouraged job applicants from pursuing employment with federal agencies or contractors and deprived the federal government of needed talent. The financial costs of lengthy security clearance processes are eventually passed from contractors to the federal government and the U.S. taxpayer.

Consistency of standards and reciprocity. One of the earliest issues that Congress pursued with regard to security clearances was that of ensuring consistency of standards across government agencies. This concern persists. For example, a 1983 GAO report pointed to the need for the Navy to require consistency across its different commands in adjudicating security clearances, while an April 2001 GAO report called for more consistency across the entire DOD.[18]

Since the attacks of September 11, 2001, Congress has called for government-wide consistency that would permit full reciprocity, that is, that all clearances issued by authorized agencies across the U.S. Government would be accepted by all other agencies. Heightened awareness after 9/11 of the need for elements of the Intelligence Community and law enforcement to share information and to work together increased the urgency of reforming the security clearance process.

Congress has been particularly concerned about cases in which federal government employees and contractors who are moving or are detailed from one government agency to another have been required to undergo lengthy reinvestigations and adjudications by a new employer. While Congress has sometimes framed this as one aspect of the timeliness problem, it has increasingly focused on issues of interagency reciprocity in its own right.

In 2006, the Oversight and Investigations Subcommittee of the House Permanent Select Committee on Intelligence conducted a review of IRTPA implementation and published its findings. With regard to security clearances, the Oversight and Investigations Subcommittee acknowledged improvements in clearance timeliness, but it found little progress in other areas. According to the report, the DNI had done little to ensure reciprocity and had no way of measuring progress toward that goal. In response, ODNI staff pledged to be more proactive, and said that new guidance would be issued in 2006 to replace the outdated Director of Central Intelligence Directive (DCID) 6/4.[19] Intelligence Community Directive 704, the intended replacement for DCID 6/4, has still not been issued.

Quality. GAO reports have repeatedly urged greater attention to quality of the investigation and adjudication processes. Problems such as inadequate training of adjudicators and infrequent reinvestigation of existing clearance holders have been cited over the years. Lack of confidence in the quality of clearance processes has often been cited as an impediment to full reciprocity in accepting

---

[17] GAO. Report to Congressional Requesters. "DOD Personnel Clearances: Additional OMB Actions Are Needed to Improve the Security Clearance Process. GAO–06–1070. September, 2006.

[18] GGD–83–66 and GAO–01–465.

[19] Director of Central Intelligence Directive 6/4, Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI).

security clearances granted by other agencies. Clear metrics on quality would increase confidence in the security clearance process across agencies. Backlogs can sometimes result in reduced rigor. For example, in the 1990s, GAO reported cases in which long delays in completing security clearances led agencies to waive investigative requirements. In a 1999 report to the Ranking Member of the House Armed Services Committee, GAO reported that 92% of background investigations were deficient in one investigative area, 77% were deficient in multiple areas, and 16% of investigations failed to pursue information about an applicant's criminal history, alcohol or drug use, financial trouble, or other significant problems.[20]

Recently, the Subcommittee urged OMB, which in 2005 assumed responsibility for overall management and policy for security clearances, to focus more attention on issues of quality and to establish clear metrics for quality of security clearance investigations and adjudications.

Workforce diversity. Analyses of Intelligence Community performance immediately preceding the attacks of September 11, 2001, brought public attention to the lack of personnel with diverse language skills and cultural backgrounds. The 9/11 Commission Report made it clear that, because very few American colleges or universities offered programs in Middle Eastern languages or Islamic studies, the Intelligence Community needed urgently to recruit personnel from among first- or second-generation Americans with the needed backgrounds.[21] However, the report also found that the clearance process was hindering the Intelligence Community's ability to hire people with the needed expertise:

> Security concerns also increased the difficulty of recruiting officers qualified for counterterrorism. . . . Many who had traveled much outside the United States could expect a very long wait for initial clearance. Anyone who was foreign-born or had numerous relatives abroad was well-advised not even to apply.[22]

The clearance process that had been designed to weed out applicants with relationships to hostile foreign nationals was preventing the hiring of applicants whose knowledge of foreign languages and cultures could help protect the United States from terrorist threats. This recruiting barrier has become a principal bipartisan concern that has prompted legislative provisions calling for "multi-level security clearances" in the intelligence authorizations bills for FY 2006 through FY 2009.

VIEWS OF INDUSTRY

Private firms carrying out contracts for DOD and the Intelligence Community have provided Congress useful information about the state of the security clearance process. They, along with other private firms who support the security clearance process itself, have

[20] GAO. Report to the Ranking Minority Member, Committee on Armed Services, House of Representatives. "DOD Personnel: Inadequate Personnel Security Investigations Pose National Security Risks." GAO–04–344. May 26, 2004.

[21] The National Commission on Terrorist Attacks Upon the United States. "The 9/11 Commission Report." July 22, 2004.

[22] Ibid.

also offered valuable insights into the ways in which the process might be updated.

Across the government, employees working on federal contracts and as individual contractors hold many of the security clearances. A 2004 report by GAO found that nearly one-third of DOD-issued clearances, nearly 700,000 out of two million, were held by industry personnel.[23] These contracts can be vital to the success of the defense and intelligence missions, as contractors provide valuable personal services as well as technical and industrial expertise.

For corporations working on intelligence contracts, long processing times for security clearances can have serious staffing and schedule implications. Representatives of industry have told the subcommittee that delays in putting personnel to work on federal contracts can cause cost and schedule overruns for the contracting agency. Ultimately, these costs are borne by taxpayers. The problem is even greater for small businesses, which may lack the cleared staff required to review classified requests for proposals, and therefore cannot compete for contracts.[24]

The 2004 GAO report cited above found that DOD's clearance process was not fit to provide high-quality, prompt clearance determinations for industry personnel. As of March 2004, DOD had a backlog of 188,000 defense industry clearance cases and an average processing time of 375 days. In light of the large backlogs and severe delays experienced by industry personnel, DOD considered the option of establishing a single adjudicative facility for industry. In 2007, a working group of government and industry representatives was created to monitor industry clearance timeliness and provide recommendations on improvements. The working group expressed concern about the timeliness of industrial clearances, and reported that 80% of clearance requests were not acted upon within an average of 120 days and that adjudication times were lengthening.[25]

Even though the timeliness of security processing has improved greatly across all levels of clearances, clearances for industry personnel still take longer than those for government employees. In the first quarter of FY 2008, for example, the average time required by the most timely 80% of the clearances for DOD military and civilian employees was 104 days, while the time required for the comparable group of DOD industry personnel was 151 days.[26]

Industry groups have grown more vocal about the need for change in the personnel security system. In 2007, the Intelligence and National Security Alliance (INSA), a professional organization of industry representatives, intelligence employees, and academics, published a white paper on reforming the clearance system.[27] The INSA paper argued that the system is weighted so heavily toward keeping dangerous individuals out, that it fails to allow in the right individuals. The system is outdated, Cold War-oriented, and technologically backward. The clearance regime's administrative, investigative, and adjudicative techniques are stuck in decades past, and

[23] GAO–04–632.

[24] Informal round-table discussions held by Subcommittee on Intelligence Community Management on June 15, 2007, and related staff conversations.

[25] Office of Management and Budget. "Report of the Security Clearance Oversight Group." February 14, 2008.

[26] Ibid.

[27] Intelligence and National Security Alliance Council on Security and Counterintelligence. "Improving Security While Managing Risk: How Our Personnel Security System Can Work Better, Faster, and More Efficiently." October 2007.

need to be adapted to the social ramifications of our mobile, networked, and dynamic, culture. The system is keeping out first- and second-generation Americans and other potential employees. Furthermore, industrial security clearance delays and backlogs have made clearance holders a commodity, driving up the cost of government contracts. According to INSA, use of commercial databases in investigations, end-to-end automation, and especially a shift in emphasis from up-front investigations to a continuous monitoring of personnel who hold clearances, are all necessary to reform the system.

REQUIREMENTS OF THE INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004

Citing the need for a fundamental restructuring of the Intelligence Community in the wake of the 9/11 terrorist attacks and the new challenges posed by terrorism and other 21st century threats, Congress approved the IRTPA,[28] the most comprehensive reform of the Intelligence Community since its creation over a half century earlier. Principal among the congressionally mandated changes was the establishment of a new position of Director of National Intelligence (DNI), with strengthened authorities to centralize and unify control over a community long viewed as more of a loose confederation of 16 separate intelligence entities than as an integrated Intelligence Community.

By centralizing authority over the Intelligence Community, Congress attempted to address one of the principal problems underscored by the 9/11 Commission, which likened the elements of the Intelligence Community to a set of specialists in a hospital, each ordering tests, looking for symptoms, and prescribing medications.[29] What was missing, according to the 9/11 Commission, was an attending physician to make sure they work as a team. As outlined by Congress, the job of the DNI was to be the "attending physician," with the authority to make sure the Intelligence Community works as a team to confront terrorism and the other emerging threats of the 21st century, threats the 9/11 Commission said increasingly called for quick, imaginative, and agile responses.[30]

One of a number of problems Congress expected the DNI to confront with his new authorities was that of the security clearance process, often criticized as typifying what the 9/11 Commission characterized as an Intelligence Community that had become "too complex and secret."[31] In Title III of IRTPA, Congress sought "to bring greater efficiency, speed, and interagency reciprocity to the security clearance process."[32] A key feature is the centralization of responsibility for security clearances.

The following paragraphs set forth the main provisions of Title III of the Act. Implementation of the provisions is discussed later in greater detail.

Uniform policies and unity of responsibility. Section 3001(b) of IRTPA requires that, within 90 days of enactment, the President

[28] P.L. 108–458, Dec. 17, 2004.
[29] The 9/11 Commission Report, p. 353.
[30] Ibid, p. 399.
[31] Ibid, p. 410.
[32] Conference report to accompany S. 2845, Intelligence Reform and Terrorism Prevention Act of 2004, December 7, 2004 Title III.

make one entity responsible for "directing day-to-day oversight of investigations and adjudications" of security clearances throughout the U.S. Government. That entity is charged with developing and implementing "uniform and consistent policies and procedures to ensure the . . . timely completion" of all clearances. It has the final word in authorizing agencies to conduct investigations and to adjudicate clearances.

Under Section 3001(c), the President was required, within 180 days of enactment, to "select a single agency . . . to conduct, to the maximum extent practicable, security clearance investigations" of all employees and contractor personnel "and to provide and maintain all security clearances of such employees and contractor personnel."

Reciprocity. Section 3001(d) requires, "All security clearance background investigations and determinations completed by an authorized investigative agency or authorized adjudicative agency shall be accepted by all agencies." This language specifies that "determinations" as well as "investigations" by one agency shall be accepted by all other agencies.

Database on security clearances. Section 3001(e) requires that, within a year, OPM is to establish and have operating an integrated, secure database that integrates data relevant to security clearances for all government employees and contractors. This database shall integrate information from all other federal clearance tracking systems. Each agency must check the database to determine whether an individual requiring a security clearance has already been granted or denied one or had one revoked. To enforce this provision, the extent to which an agency is submitting information to this database will be evaluated and this will help determine whether to certify the agency as an authorized investigative or adjudicative agency.

Use of information technology. Section 3001(f) requires the policy oversight entity to evaluate the use of available information technologies and databases for expediting investigative and adjudicative processes, doing ongoing verification of personnel with clearances; or augmenting periodic reinvestigations. The law requires that, no later than a year after enactment, the policy oversight entity submit a report to the President and Congress on the results of this evaluation.

Reduction in the length of the clearance process. The most frequently-referenced requirements of Title III are in Section 3001(g). These include a plan, to be developed by the policy oversight entity within 90 days after that entity is selected, to reduce the length of the personnel security clearance process. The plan is to be developed in consultation with the appropriate committees in Congress and each authorized adjudicative agency, and is to take effect five years after enactment. "To the extent practical the plan . . . shall require that each authorized adjudicative agency make a determination on at least 90 percent of applications for a personnel security clearance within an average of 60 days after . . . receipt of a completed application," or 40 days for investigation and 20 for adjudication. An interim standard, to be met not later than 2 years after enactment, is that each agency shall make a determination on at least 80 percent of applications with an average of 120 days after receiving the application.

Annual progress reports. Under Section 3001(h), the policy oversight entity is to submit progress reports by February 15, 2006, and annually through 2011.

IMPLEMENTATION AUTHORITIES AND PLANS

E.O. 13881, issued June 27, 2005, in response to the requirements of IRTPA's Title III, affirmed a policy that "agency functions relating to determining eligibility for access to classified national security information shall be appropriately uniform, centralized, efficient, effective, timely, and reciprocal." It gave OMB the authority to assure implementation of that policy. Pursuant to that authority, OMB delegated to OPM the central role for security clearance investigations called for in Title III, Section 3001(c).

On June 30, 2008, E.O. 13381 was replaced by E.O. 13467, a new executive order reforming clearance processes and formalizing a new governance structure for the processes of hiring and clearing federal government personnel. The Joint Security and Suitability Reform Team proposed a governance structure, including a Performance Accountability Council, which is a collaborative effort consisting of representatives of DOD, OMB, DNI, and OPM. The new council is to be accountable for achieving the goals of security clearance reform. To be chaired by OMB's Deputy Director for Management, the Council includes the DNI as the "Security Executive Agent" responsible for security clearances government-wide; and affirms the Director of OPM as responsible for the federal government's workforce.

In April 2007, DNI Mike McConnell issued the United States Intelligence Community 100-Day Plan for Integration and Collaboration. The plan committed the Intelligence Community to a "culture of collaboration," to "modernize business practices" and to "accelerate information sharing," among other broad objectives intended to overcome the obstacles to interagency collaboration on security issues identified following the attacks of 9/11.

One specific problem targeted in the DNI's 100-Day Plan was that "multiple, complex and inconsistent security clearance systems slow the pace in filling open positions and moving personnel." The plan envisioned "timely granting of clearances and the ability to enter all IC agencies with the IC One Badge without having to send clearances." At the end of the 100-day period, the DNI reported having taken a first step by developing "a pilot program that will pave the way for a standard and uniform clearance process. . . ."[33]

A 500-Day Plan for Integration and Collaboration, which the DNI issued in October 2007 and would extend until the end of the current administration, outlined a strategy to deliver an "end to end security clearance process" in which the "performance of IC agency personnel security programs meet or exceed IRTPA guidelines for clearance case processing times." The new plan, however, made no reference to an "IC One Badge" that would be accepted by all agencies.

[33] Follow-Up Report, July 27, 2007.

ASSESSING PERFORMANCE AGAINST IRTPA REQUIREMENTS

One entity responsible for uniform policies and implementation. Actions have been taken, but in practice, the requirement has not been fully met. The principal provision of this section, the selection of OMB as the lead entity, was implemented through E. O. 13381, which the President issued approximately 190 days after the law's enactment.[34] That order was replaced on June 30, 2008, by E.O. 13467, which has taken a different approach to implementing this IRTPA provision, as discussed below.

To implement IRTPA'S requirement that the entity selected be "the final authority to designate an authorized investigative agency or authorized adjudicative agency," E.O. 13381 specified that the Director of OMB might assign to any agency any process relating to determinations of eligibility, and that OMB was to supervise the agencies in carrying out the investigatory or adjudicatory activities. The E.O. authorized OMB, after consulting with the Secretary of Defense, the DNI, and certain other department heads, to issue guidelines to the agencies "to ensure appropriate uniformity, centralization, efficiency, effectiveness, and timeliness in processes relating to determinations by agencies of eligibility for access to classified national security information."

In practice, the centralization of authority required by the law has not been fully realized. OMB's policy oversight has not succeeded in setting forth a consistent interpretation of interagency reciprocity, nor has it ensured implementation of other Title III requirements.

The new executive order, E.O. 13467, replaces OMB as the central authority with a committee, the Suitability and Security Clearance Performance Accountability Council ("the Council"). The Council's members include the Director of OPM and the DNI, and it is chaired by OMB's Deputy Director for Management. The Council is accountable for "aligning" executive branch policies and procedures regarding security and suitability clearances. The specific responsibilities for policy and oversight of the security clearance process, which had been assigned to OMB, are now assigned to the DNI. These include the responsibility to designate agencies to conduct security investigations and to "ensure reciprocal recognition of eligibility for access to classified information among the agencies."

By naming the DNI as the "Security Executive Agent," the new executive order may make it possible to achieve greater alignment of policies regarding Sensitive Compartmented Information (SCI). E.O. 13381 had restricted OMB's authority with regard to certain types of access. For determining access to SCI and intelligence-related Special Activity Programs (SAPs), OMB would have required the concurrence of the DNI; while OMB guidelines on non-intelligence (military operational, strategic and tactical) SAPs would have required the concurrence of the head of the agency responsible for that program.

A single entity for investigations. This provision, which requires that a single agency shall, "to the maximum extent practicable," be responsible for conducting security clearance investigations, has been partially implemented. The statute also requires this entity to

[34] The law required this selection within 90 days of enactment.

integrate security clearance applications, investigations, and determinations into a database, and ensure security clearance investigations are conducted under uniform standards and requirements.

In practical terms, OPM is this single entity because it conducts 90% of the background investigations for security clearances, and has done so since 2005. Prior to that, these investigations were conducted by DOD. The shift from DOD to OPM was authorized by Congress in the National Defense Authorization Act for FY 2003, and occurred in 2005. In addition, in June 2005, OMB designated OPM as the single entity responsible for security clearance investigations.[35]

OPM has not fully exercised the government-wide management role for the other requirements of this section, nor does the OMB designation make reference to these other requirements. Although IRTPA calls on "the selected agency" to integrate the work related to security clearances across the government, in practice, OPM's role is limited to providing investigative services to DOD and certain other agencies.[36] Rather than "provide and maintain all security clearances . . ." and "integrate reporting of security clearance applications, security clearance investigations and determinations," into a single database, OPM maintains records only of the clearances for which it provides the investigations. It does not even maintain records of the number of cases investigated or adjudicated by other agencies.[37]

While the federal government had standards for investigation and adjudication prior to IRTPA, OPM did not issue new guidance under the statute. However, E.O. 13467 issued in 2008, creates a Security Executive Agent who will have responsibility for "developing uniform and consistent policies and procedures" for investigations and adjudications. Under the executive order the Security Executive Agent is the DNI. On September 17, 2008, the DNI's representative testified to the Subcommittee that a review of the policies and procedures for investigations and adjudications is underway.

Reciprocity. Under IRTPA, "all security clearance background investigations and determinations completed by an authorized investigative agency or authorized adjudicative agency shall be accepted by all agencies." This standard has not been met.

The law specifies that in determining whether to grant a clearance to someone who already has the same level clearance from another agency, no new investigations may be required; and there may be no additional investigative or adjudicative requirements, other than a requirement of a polygraph examination, that exceed requirements specified in the executive orders establishing those security requirements. The section provides, however, for the head of the policy oversight entity to make exceptions necessary for national security purposes.

---

[35] June 30, 2005, OMB Memorandum for Heads of Executive Departments and Agencies, "Allocation of Responsibilities for Security Clearances under the Executive Order, Strengthening Processes Relating to Determining Eligibility for Access to Classified National Security Information."

[36] "OPM provides background investigation products and services to agencies to assist them with making security clearance or suitability decisions . . ." Ibid.

[37] In response to ICM staff phone request for information about the number of security clearances across the Federal Government, an OPM legislative affairs officer said, "We have information only about the clearances that we (at OPM) do." Phone conversation, July 18, 2008.

The interpretation and application of reciprocity by the current Administration has been inconsistent.

• Presidential guidance on reciprocity has changed over time. E.O. 12968, issued August 2, 1995, required that background investigations and eligibility determinations would be reciprocal. E.O. 13381 issued in June 2005 loosened the standard so that only "agency functions relating to determining eligibility for access" would be reciprocal, without requiring that final determinations be accepted. Then, in June 2008, E.O. 13467 went back to the stronger language in the 1995 order, requiring that "background investigations and adjudications shall be mutually and reciprocally accepted by all agencies." [38]

• In July 2007, the DNI suggested that agencies would not re-adjudicate clearances that have already been granted by other agencies when he described the goal of "modernizing business practices" in security clearances as the "timely granting of clearances and the ability to enter all IC agencies with the IC One Badge . . ."

• In testimony to the Subcommittee, Administration witnesses argued that each agency should adjudicate clearances for its own personnel. At the Subcommittee's open hearing on February 27, 2008, Mr. Clay Johnson, OMB Deputy Director for Management, testified, "If you asked . . . anybody in the executive branch, senior capacity, whether your access to Top Secret information at Interior would qualify you for access to Top Secret information at CIA, you would hear a resounding 'no.'" Ambassador Eric Boswell, then Assistant Deputy Director of National Intelligence for Security, explained that a condition of employment at an intelligence agency is that everyone is cleared at the Top Secret level and has SCI access. Thus, the security clearance process is indistinguishable from the determination that the applicant is suitable for employment at that agency. Mr. Johnson testified to the Subcommittee at its September 17, 2008, open hearing that the final determination for suitability and access to secure information ought to be made by the agency that is employing the person.

• Even today, the Administration acknowledges exceptions to reciprocity. Pressed by ICM members at their September 2008 hearing about the extent of reciprocity in adjudications, Mr. Johnson and other Administration witnesses indicated that OMB allows four reasons for which agencies may determine not to recognize a clearance issued by another agency: 1) if the position requires a polygraph and the applicant's current position does not; 2) if the existing clearance was issued as an interim clearance; 3) if the position requires adjudication of foreign national family members issues, which were not made earlier; and 4) if the job requires disqualifying applicants because of certain disqualifying conduct.

The standard for reciprocity set by the law contains some ambiguity. The law could be interpreted to require that one agency's Top Secret clearance must be automatically recognized by all other agencies as though the bearer of that clearance were wearing the "IC One Badge." Alternatively, reciprocity might mean that, when one agency considers whether to provide a security clearance to

[38] 38 E.O. 13467, Section 2.1(c). Section 3(c) of this Order states that the Order does not supersede the provisions in the 1995 Order cited above.

someone already holding a clearance, the agency must accept the existing clearance unless it falls into one of the four listed exceptions. Or reciprocity might be interpreted to mean only that when the receiving agency adjudicates the security clearance, it must not re-do the existing investigatory work or revisit the particular issues that were considered previously in reaching the security clearance determination.

OPM's role as investigator for the vast majority of clearances means that investigative reciprocity is less of an issue than adjudicative reciprocity. There is no definitive information on the actual practice of the intelligence agencies with regard to accepting each other's security adjudications. Senior officials have insisted that each agency readily accepts clearances adjudicated by the others. However, no measures exist to substantiate that claim. At the Subcommittee's hearing on September 17, 2008, Mr. Johnson acknowledged, "We don't have metrics for measuring reciprocity. We rely on anecdotal evidence. We poll the contractor community and we notice trends in the anecdotal reporting of nonreciprocal behavior." [39]

Concerned by persistent anecdotal information about cases in which reciprocity appears not to have been the rule, the House Permanent Select Committee on Intelligence included in the FY 2009 authorization bill a provision requiring the Inspector General of the Intelligence Community to audit security clearance reciprocity in the Intelligence Community.

An integrated, secure database. The law calls for a database "into which appropriate data . . . shall be entered from all authorized investigative and adjudicative agencies." This requirement has not been met.

At present, there are two separate databases, the Joint Personnel Adjudication System (JPAS), which covers DOD, and Scattered Castles, used by the Intelligence Community. Moreover, JPAS does not include data about clearances that are not investigated by OPM, such as the Department of Homeland Security and the Department of State, which are maintained in other databases.

At an ICM hearing held on February 27, 2008, the OPM witness reported that OPM and DOD had linked their databases in order to ensure "that database is made accessible across the government to all agencies." However, she noted, "Now, it does not include the clearances in the Intelligence Community. If we had tied those systems together, it would have made the whole system classified, and then it would not be usable to a broad section of the government." [40]

At the same hearing, Mr. Eric Boswell, then-Assistant Deputy Director of National Intelligence for Security, added, "The IC is served by one common database. . . . It is a classified database, for good reasons." Reflecting on this situation, he acknowledged, "Reciprocity is not well served by the existing IT structure. We are working, in the Joint Team, to try to find some way to make that happen."

---

[39] Testimony of Mr. Clay Johnson, Deputy Director, OMB, before the Subcommittee, September 17, 2008.

[40] Testimony of Kathy L. Dillaman, Associate Director, Federal Investigative Services Division, OPM, before Subcommittee on Intelligence Community Management of the House Permanent Select Committee on Intelligence, June 27, 2008.

The provision in this subsection requiring OMB to "evaluate the extent to which an agency is submitting information to, and requesting information from, the database . . . as part of a determination of whether to certify the agency as an authorized investigative agency or authorized adjudicative agency" appears not to have been applied.

Evaluating the use of information technology. This requirement has been met, though belatedly. A report about the results of an evaluation of the use of available IT to expedite clearance processes was to be submitted by December 2005. As of 2008, no such report had been produced.

As a complement to the April 2008 Joint Reform Team report, the team prepared an appendix outlining the purpose, methods, and key findings of pilot programs that examined potential changes to the clearance system.[41] Many of these pilot programs evaluated the application of modern IT systems to the clearance process. Until very recently, all fingerprints were taken with ink, applications filled out on paper, and every stage of every investigation and adjudication, no matter how simple, conducted by security personnel. The demonstrations evaluated automated or electronic approaches to these tasks.

These IT systems have been tested and proven independently of each other. The outdated processes are now being replaced. Testifying at the Subcommittee's September 17, 2008 hearing, the OPM witness reported that "94 percent, almost all, of submissions [to OPM] for national security investigations were done electronically, and almost half of the fingerprints were captured using digital capturing equipment."[42] The next critical step is to test these systems as part of an end-to-end process to ensure that they work together seamlessly. Such a demonstration is scheduled to take place by the end of 2008.[43] Although the undertaking of this evaluation is belated, the Subcommittee applauds the effort and looks forward to reviewing the results.

Reduction in the length of the clearance process. IRTPA specified that within two years of enactment each authorized adjudicative agency shall make a determination on at least 80% of all applications for a personnel security clearance within an average of 120 days from the date the investigative agency receives the application. The language further stipulated that the 120 days should allow no more than 90 days for the investigative phase and no more than 30 days for the adjudicative phase.

The Administration reported that this interim standard had been met on average across the adjudicating agencies. However, their data suggests that this standard was not met by each agency. Moreover, its presentation creates the best possible picture from what is, upon closer inspection, a mixed record. For example, in order to argue that the security clearances for which OPM conducts investigations had met the IRTPA standard, the report: 1) considered only the adjudications begun and reported during the first

[41] Appendix to the Security and Suitability Process Reform Initial Report, 30 April 2008: Demonstration Activity Results, 19 June 2008.

[42] Testimony of Ms. Kathy Dillaman, Associate Director for Federal Investigative Services, OPM, before the Subcommittee on Intelligence Community Management on September 17, 2008.

[43] Testimony of Ms. Elizabeth McGrath, Principal Deputy Under Secretary of Defense for Business Transformation, before the Subcommittee on Intelligence Community Management on September 17, 2008.

quarter of FY 2007; 2) considered only initial investigations, not reinvestigations; 3) did not include "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";[44] and 4) interpreted the standard as requiring no more than 90 days for investigations and 30 days for adjudications, ignoring the requirement that the total amount of time for the security clearance process should not exceed 120 days.

It should be noted that the requirements for timeliness in IRTPA also lack specificity in some regards. For example, the law aggregates TS-level clearances with those at the Secret and Confidential level. More meaningful measures of progress would consider the timeliness of the TS-level clearances separately. Also, since the law does not mention the time to transmit an application to OPM from the agency that receives the application, the Administration reinterpreted the IRTPA standard of 120 days to mean 130 days for "end-to-end" processing, including a period of 14 days for initial transmission of the application, 25 days for adjudication, and 91 days for investigation.[45]

Nevertheless, the improvement in timeliness achieved by the December 2006 interim deadline was a remarkable achievement, particularly by OPM, which had inherited large backlogs in 2005. Looking at the timeliness of the investigation phase for initial clearances, the average for 80% of all those completed during the first quarter of FY 2007 was 101 days. While this average falls short of the IRTPA standard of 90 days for investigations, it shows marked progress over previous years. While initial investigations for clearances at the TS level required 392 days in FY 2004 and 347 days in FY 2005, in FY 2006 they were completed, on average, in 286 days. For Secret/Confidential levels, the required time was reduced from an average of 179 days in FY 2004 to 155 days and 157 days in FY 2005 and FY 2006, respectively.[46]

Across the federal government, performance against the interim IRTPA standards was uneven:

- The adjudications by agencies whose investigations are performed by OPM averaged 39 days, falling short of the IRTPA standard of 30 days.
- Data from the individual agencies of the Intelligence Community was not provided, but the Intelligence Community as a whole appears to have met or exceeded the standard. On average, 83% of all investigations and adjudications that were completed in the first quarter of FY 2007 and the preceding fiscal year took 103 days to process.[47] This figure does not include the time for initial transmittal and other processing, which would be counted in an end-to-end measurement.
- The agencies outside of the Intelligence Community that conduct their own investigations showed mixed results. The State Department exceeded the IRTPA standard, requiring an average of

[44] Ibid., p.1.
[45] Ibid., footnote 1.
[46] Ibid., p.1.
[47] Report of the Security Clearance Oversight Group Consistent with Title III of the Intelligence Reform and Terrorism Prevention Act of 2004, February 2007, p.5.

only 51 days to accomplish both the investigation and adjudication. Data was insufficient to report on Department of Homeland Security performance, although the units that reported fell short of the IRTPA standard. The Department of Justice/FBI performance fell well short of the IRTPA standard for investigation, although it conducted adjudications in less time than the IRTPA standard.

The second set of milestones established under IRTPA will come due in December 2009. At that point, 90% of all applications are to be processed within an average of 60 days. Given past performance, meeting that standard will pose a significant challenge for almost all agencies. In an effort to move toward those standards, in February 2008, the Security Clearance Oversight Group set goals to be met by September 2008, including:

- providing initial security clearances to 90% of industry employees in same time it takes to provide them to non-industry employees;
- 90% of TS initial investigations in less than 90 days; and
- 90% of Secret/Confidential initial investigations in less than 65 days.

Annual progress reports. In February 2007 and February 2008, OMB submitted to Congress the annual reports required under this section. These provide detailed information about progress achieved in reducing the processing time for security clearances. The February 2007 report also describes efforts to improve reciprocity, a subject that is absent from the February 2008 report.

CURRENT REFORMS: ISSUES FOR OVERSIGHT

The Subcommittee remains concerned that the process has been driving with the emergency brake on, and that four years after IRTPA, the clearance process has not been dramatically streamlined, but instead consists of layers and layers of planning.[48] The Subcommittee has been troubled by the quality of the security clearance process. It has pressed OMB repeatedly and unsuccessfully to establish metrics for the quality of security clearance investigations and adjudications. Without clearly established methods of evaluating and assessing the security clearance process, there is no way to ensure that the process reaches the intended result of providing access to trustworthy Americans while protecting our national security.

The lack of full reciprocity among agencies continues to exact financial costs across the government and the contracting community, as well as the intangible cost of lost opportunities for collaboration. Members of the Subcommittee expressed dismay that, despite Congress's intent to bring the security clearance process under a single authority, information and authority remain so dispersed that no one knows how many people in the U.S. Government hold security clearances.[49] As the Ranking Member has stated, "The problems with security clearance reform do not seem to be ones of money or even ideas. The real issues seem to be stubbornness and a refusal to embrace system-wide efficiency over agencies' proprietary desire to control the clearance process."[50]

---

[48] Subcommittee Chairwoman Eshoo, July 30, 2008, hearing of the Subcommittee on Intelligence Community Management of the House Permanent Select Committee on Intelligence.

[49] Ibid.

[50] Ibid, opening statement of Ranking Member Darrell Issa, July 30, 2008.

In March 2008, the Committee formally requested that GAO conduct its first assessment of the security clearance process in the Intelligence Community. This study, to be completed in the fall of 2008, includes an evaluation of the ongoing joint pilot reform effort being conducted by the DNI and DOD and a review of the criteria that the administration is using to assess the effectiveness of its efforts.

On July 30, 2008, the Subcommittee held an open hearing to receive preliminary results of GAO's review and to consider the impact of the Administration's new reform plan on the security clearance reform process.[51] The sole witness was GAO's Director for Military and Civilian Personnel and Medical Readiness, Defense Capabilities and Management, Ms. Brenda Farrell. Ms. Farrell based her remarks on GAO's initial review of the reform plan and the new executive order, as well as GAO's prior work on security clearance processes and its knowledge of best practices in organizational transformation.

In her testimony, Ms. Farrell emphasized that the new reform plan, unlike the plan issued in 2005 as required by IRTPA, identifies some near-term actions. She also underscored the importance, as in any major organizational change, of ensuring the full support of senior officials and the significance of the collaboration among the DNI, DOD, OMB, and OPM. She noted that such collaboration did not exist in 2005. However, she found the new plan, like the previous plan, deficient with regard to setting specific interim goals and metrics with which to track the progress of the reform effort.

GAO's review will focus particularly on the structure and role of the Performance Accountability Council created by the E.O. 13467. In her testimony, Ms. Farrell expressed the GAO's intention to evaluate OMB's role as chair of the Council and the DNI's functions as Executive Agent for security clearances and as a member of that council.[52] GAO will address how best to achieve full reciprocity of security clearances across the U.S. Government, including an assessment of the willingness of the elements of the Intelligence Community to establish a cross-agency clearance database.[53]

The Subcommittee discussed the results of the GAO study at its September 17, 2008, at which the responsible leaders of the key institutions, including the DNI, DOD, OMB and OPM, testified.

As the Subcommittee concludes its security clearance oversight activities during the 110th Congress, it finds that progress over the past five years has been disappointing. Recognizing that security clearance reform is one of the most vital workforces issues facing the Intelligence Community today, the Subcommittee remains committed, on a bipartisan basis, to ensuring that the relevant agencies fully accomplish the mission of reform.

It is the intention of the Subcommittee to hold hearings on legislative proposals early in the 111th Congress that would spur security clearance reform by requiring agencies to report to Congress on key metrics on the security clearance process. A standard meth-

[51] "Security and Suitability Process Reform," April 30, 2008, Initial Report of Joint Security and Suitability Reform Team; and E.O. 13467, issued June 30, 2008.

[52] Testimony of Ms. Brenda Farrell, Director, Defense Capabilities and Management, GAO, before Subcommittee, July 30, 2008.

[53] Ibid.

od of evaluation would allow tracking of improvements from year to year and enable agencies to judge the effectiveness of one another's security clearance process, thereby improving confidence in the system. The legislation would also clarify congressional intent concerning the meaning of reciprocity and the degree to which responsibility for security clearance adjudications must be consolidated.

○