S. Hrg. 110–338

EVALUATING THE PROGRESS AND IDENTIFYING OBSTACLES IN IMPROVING THE FEDERAL GOVERNMENT'S SECURITY CLEARANCE PROCESS

HEARING

BEFORE THE

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

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

MAY 17, 2007

Available via http://www.access.gpo.gov/congress/senate

Printed for the use of the Committee on Homeland Security
and Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE
35–535 PDF WASHINGTON : 2008

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

JOSEPH I. LIEBERMAN, Connecticut, *Chairman*

CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
THOMAS R. CARPER, Delaware
MARK L. PRYOR, Arkansas
MARY L. LANDRIEU, Louisiana
BARACK OBAMA, Illinois
CLAIRE McCASKILL, Missouri
JON TESTER, Montana

SUSAN M. COLLINS, Maine
TED STEVENS, Alaska
GEORGE V. VOINOVICH, Ohio
NORM COLEMAN, Minnesota
TOM COBURN, Oklahoma
PETE V. DOMENICI, New Mexico
JOHN WARNER, Virginia
JOHN E. SUNUNU, New Hampshire

Michael L. Alexander, *Staff Director*
Brandon L. Milhorn, *Minority Staff Director and Chief Counsel*
Trina Driessnack Tyrer, *Chief Clerk*

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

DANIEL K. AKAKA, Hawaii, *Chairman*

CARL LEVIN, Michigan
THOMAS R. CARPER, Delaware
MARK L. PRYOR, Arkansas
MARY L. LANDRIEU, Louisiana

GEORGE V. VOINOVICH, Ohio
TED STEVENS, Alaska
TOM COBURN, Oklahoma
JOHN WARNER, Virginia

Richard J. Kessler, *Staff Director*
Evan Cash, *Professional Staff Member*
Jennifer A. Hemingway, *Minority Staff Director*
David Cole, *Minority Professional Staff Member*
Emily Marthaler, *Chief Clerk*

CONTENTS

WITNESSES

THURSDAY, MAY 17, 2007

ALPHABETICAL LIST OF WITNESSES

APPENDIX

EVALUATING THE PROGRESS AND IDENTIFYING OBSTACLES IN IMPROVING THE FEDERAL GOVERNMENT'S SECURITY CLEARANCE PROCESS

THURSDAY, MAY 17, 2007

U.S. SENATE,
SUBCOMMITTEE ON OVERSIGHT OF GOVERNMENT
MANAGEMENT, THE FEDERAL WORKFORCE,
AND THE DISTRICT OF COLUMBIA,
OF THE COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Subcommittee met, pursuant to notice, at 9:42 a.m., in Room 342, Dirksen Senate Office Building, Hon. Daniel K. Akaka, Chairman of the Subcommittee, presiding.

Present: Senators Akaka and Voinovich.

OPENING STATEMENT OF SENATOR VOINOVICH

Senator VOINOVICH [presiding]. The meeting will please come to order. Senator Akaka is on his way. He had a speech this morning, and I know how those go.

I want to first of all thank Senator Akaka for holding this Subcommittee's fourth hearing on the Federal Government's security clearance process. Although I am no longer the Chairman of this Subcommittee and am now Ranking Member, Senator Akaka and I collaborated during the 109th Congress that this issue is very important to the future of our country. I am very grateful to him that we are continuing our oversight on the security clearance process.

Our oversight work on the security clearance process began during the 109th Congress because of our concern with the long-standing backlog with security clearances and the cumbersome process that hampered the Federal Government's ability to clear highly-skilled employees in a timely manner. Our clearance processing system remains broken! It remains broken, limiting the ability of our national security agencies to meet their heightened mission requirements.

The impact of a flawed clearance system is not limited to Washington. For example, during a recent visit to Wright-Patterson Air Force Base in Ohio, I was alarmed to learn of the considerable delays that continue to plague the Air Force's ability to fill critical workforce needs.

One year has passed since our last hearing. The first timeliness milestone set forth in the Intelligence Reform and Terrorism Prevention Act are behind us. In thinking about today's hearing, a number of questions come immediately to mind.

Does the current security clearance process, a Cold War relic, have the capacity to meet the security needs of our Nation? Will OPM, which is responsible for about 90 percent of all background investigations for the Federal Government, be able to meet its investigative timeliness goals in the long term? Why isn't the Department of Defense devoting the resources necessary to reform its process?

Are we taking full advantage of technology and our partners in industry to make needed improvements? I have talked to industry and they are livid about this. They can't understand why we in the Federal Government can't incorporate available technology to improve this process.

Honest responses to these questions will help us gain a better understanding of whether the current path will lead to success or failure.

My concern is not meant as a critique of the efforts of those individuals who appear before the Subcommittee today, though I have some strong words. In particular, I want to applaud Mr. Johnson for his untiring commitment to this issue. Mr. Johnson, your leadership will become even more vital to this effort as we approach the end of the Administration. A question for the Administration is, are you going to wind down or are you going to wind up?

Under the guidance of Ms. Dillaman, OPM has made noticeable improvements in the timeliness of security clearances. However, despite the progress that has been made, I still have some very serious concerns.

First, although DOD's senior leadership continues to state that they are committed to resolving the systemic problems at the Defense Security Service (DSS), actions do speak louder than words. Since her selection as permanent Director in February, DSS Director Kathy Watson has taken several important steps to reform the process, including hiring a committed, competent leadership team. This program has been on the Government Accountability Office's high-risk list for years and has led to the development of a corrective action plan.

It is my understanding that DSS is currently under-funded by $55 million for fiscal year 2007. I question how we can expect DSS to reform itself in the absence of adequate resources to get the job done, let alone build the infrastructure necessary to sustain itself in the long term.

Mr. Johnson, I expect to hear from you how this problem will be fixed, particularly since OMB has been a partner in developing the corrective action. It seems to me that if you are a partner in the corrective action, that if providing the resources is extremely important to making it happen, that the resources would be provided. It is frustrating to me that we are asking agencies to reform themselves yet we fail to provide the resources or funding to get the job done.

I had a hearing on the backlog in Social Security for folks that are making appeals on Social Security Disability and I was raising a lot of thunder. But the bottom line is, we are as guilty as they are because we haven't given them the resources to do the job. If you don't give people the funding they need, then you basically tell them that you don't think very much of the job that you are asking them to do.

Second, the February 2007 report by OMB and the Security Clearance Oversight Group identifies several obstacles which impede the security clearance process. The report admits that the Federal Government has yet to deal with the issue of reinvestigations. The OMB report also mentions the use of the e–QIP system for electronic submission of agency investigative requests. While I am pleased that the e–QIP has led to dramatic improvements in timeliness and accuracy of submissions, I remain perplexed as to why we have yet to reach 100 percent participation by agencies, including OPM. The deadline for compliance was April 2006, not April 2007. Mr. Johnson, I would like to know when you expect agencies to achieve compliance?

Third, I remain very concerned that the Federal Government under OPM's leadership is not taking advantage of innovative technology available in the marketplace. Subcommittee staff recently toured the mines in Boyers, Pennsylvania, where OPM's clearance operations center is housed. After meeting with my staff to discuss their visit, I find it hard to believe that in the year 2007, we continue to rely on a paper-intensive clearance process. Ms. Dillaman, I would like to hear from you when you expect OPM to be able to complete a fully automated investigation from start to finish?

Finally, in blatant disregard of the statute, agencies continue to disregard the reciprocity requirement. Our efforts to resolve the backlog will be diminished if agencies continue to reinvestigate and readjudicate individuals with valid clearances.

All of us here today share a common goal of fixing this process. Based on our efforts to date, we have made progress in reducing the timeliness of issuing initial security clearances, but our work is far from over. The timely hire of a highly-skilled workforce to meet our national security mission requires solutions to all the problems associated with the security clearance process. I remain committed to working on this issue until it is resolved. I remain committed to working on this issue until it is resolved.

I would like to thank our witnesses for their participation and I look forward to your testimony.

Senator Akaka has not arrived. We are going to go ahead to testimony. It is the custom of this Subcommittee that witnesses be sworn in. Will you stand and I will administer the oath to you.

Do you solemnly swear that the testimony you are about to give this Subcommittee is the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. JOHNSON. I do.

Mr. ANDREWS. I do.

Ms. DILLAMAN. I do.

Mr. STEWART. I do.

Senator VOINOVICH. Let the record show that our witnesses answered in the affirmative.

Again, I want to thank you all for being here. Mr. Johnson, we will start with your testimony.

TESTIMONY OF HON. CLAY JOHNSON, III,[1] DEPUTY DIRECTOR FOR MANAGEMENT, U.S. OFFICE OF MANAGEMENT AND BUDGET

Mr. JOHNSON. Senator, thank you very much for your commitment to this reform effort. You help us get a lot done that we wouldn't be able to get done otherwise. What I would like to do is just briefly summarize what I think we have done and not done yet.

In answer to your question, do we intend to wind down or wind up, let me put it this way. We intend and are very committed to stay tight, to remain tightly wound on this issue. This is a big priority for the government and it is a big priority for me personally because this thing can be fixed in the time that I am going to be here.

Let me tell you what I think we have done. Presently, we are investigating, completing initial clearance investigations, 80 percent of them within 90 days, as called for. It was the goal to be accomplished by December 2006. We are adjudicating 80 percent of the initial clearances in less than 30 days, which was the goal for December 2006. We have reduced the backlog of old clearances. We have unprecedented agency commitment to fix this process. We have very clear goals for each of the component parts of the process. We have the information we need to hold ourselves accountable for accomplishing those goals. We have expanded our investigation and adjudication capacity and we have begun—we are using technology to transfer information and files more quickly than before.

However, what have we not done yet? We still have a backlog of old investigations. We have not until this year begun to reform and improve the reinvestigation process. That is a commitment for 2007, a big priority for 2007. We have, as I said, focused on the two major component parts, the investigation part and the adjudication part, of the process. We are only this year creating the data information that allows us to look at the total process, from when the person submits the application to when they are told they have a job and they have a clearance. What is that total end-to-end process? There are a lot of handoffs within agencies and between agencies that don't get picked up and addressed and agencies aren't held accountable until we look at the total end-to-end. That will become a primary focus of this reform effort this year.

We have demonstrated this ability to do this in less than 90 days and adjudication in less than 30 days for several months. The proof in the pudding is can we do that over longer periods of time, and we have not—one of the challenges you raised in your opening remarks is we have not laid out what the security clearance process of the future looks like, but we are in the process of doing that and will have a very clear understanding of that by the end of this year, which we then will pick the next period of time to bring it to realization.

This year, we have established as our goals that we want to and are going to hold ourselves accountable, it is not in the legislation but we want to hold ourselves accountable for completing 85 per-

[1] The prepared statement of Mr. Johnson appears in the Appendix on page 37.

cent of all initial investigations in less than 90 days, complete 80 percent of all adjudications in less than 25 days, to complete reinvestigations in 180 days or less, to bring all record repositories up to the standard of submitting the files that are requested—90 percent of all the files that are requested within 30 days, to bring an end-to-end focus to our reform efforts so we can report not just on what adjudications are taking and not just what investigations are taking, but the total process, the process that the applicant for the security clearance, what they are realizing, and we want to explore additional—the possibility of using additional measures of investigative quality.

In answer to a couple of questions you raised in your remarks in terms of the resources for DOD, DOD was provided all the funds in the President's budget by OMB and the President provided that they requested for DSS. There have been no limitation on funds. If there is a funding issue at DSS, it is not because DOD doesn't have enough money. It is because it is not in the right place within DOD.

On the subject of e–QIP usage, yes, our commitment was—every agency's commitment was to get to 100 percent usage of e–QIP by April of last year and we didn't do it. It was not very well thought out by the agencies when they committed to do it. But the agencies on the government-wide were at 77 percent, I think, usage of it. The big agency still to get to 100 percent is DOD and they have very aggressive plans to get there by the end of this year. Our commitment is to be at 100 percent e–QIP usage by the end of this year.

In terms of the use of technology, we are not making use now of a lot of these commercially available databases that a lot of the for-profit sector is using as they grant their employees security clearances, but our R&D effort will address that and we will lay out—within the next several months, we will have R&B milestones that we will be holding ourselves accountable for by the end of 2007, 2008, and on to 2009 that we will be glad to come up here and share with you. We don't need a hearing. We will just share that with you and your staff to give you an idea about what our vision for the security clearance process of the future consists of.

That is my opening comments and I look forward to your questions.

Senator VOINOVICH. Thank you. Mr. Andrews.

TESTIMONY OF ROBERT ANDREWS,[1] DEPUTY UNDER SECRETARY OF DEFENSE FOR COUNTERINTELLIGENCE AND SECURITY, ACCOMPANIED BY KATHLEEN M. WATSON, DIRECTOR, DEFENSE SECURITY SERVICE, U.S. DEPARTMENT OF DEFENSE

Mr. ANDREWS. Good morning, sir. Thank you for the invitation to come up here this morning. I am the Deputy Under Secretary of Defense for Counterintelligence and Security and I have oversight responsibilities for DSS. I am joined by Ms. Watson, who is the Director of DSS.

[1] The prepared statement of Mr. Andrews appears in the Appendix on page 47.

Sir, I appeared here last year about 3 days after I took over my job and DSS had stopped clearances. That was not a pleasant time. I think I started my testimony by saying this is not our best day.

The crisis that led to the suspension of processing for security clearances had a cumulative effect in that it made certain that we knew that there were failures inside the system that couldn't be papered over. I can report that DSS has corrected many of the root causes of last year's shutdown, namely leadership and a lack of standard operating procedures. We have made progress to date, but much work needs to be done at DSS, throughout DOD, and across the interagency.

And let me start with the positives, what the DSS team has accomplished over the past year. A year ago, my primary concern was a failure of leadership at DSS. The outfit had gone through four directors in 5 years, all of them acting directors. In the past 4 years, they have had nine comptrollers. We have made progress, most notably in the senior team.

The Secretary of Defense named Ms. Watson as Acting Director in May 2006 and permanent Director in February of this year. Ms. Watson is the first permanent Director at the agency within the last 5 years. Kathy assembled a team, a core team, in her first few months on the job. This team is talented, focused, and committed to the success of DSS. To say that we are proud of Kathy's team would be a massive understatement, and I would like to outline some of her team's accomplishments.

We have a closer working relationship with OPM. The Defense Security Service has reinvigorated its working relationship with OPM, and together we are working to create a process to better serve our customers. We resolved the surcharge issue that existed last year. As a result of OMB mediation, we worked out an agreement with OPM over the rates that OPM charges DOD for investigations. OPM has refunded DOD $7 million in 2006 and for 2007 OPM has eliminated the surcharge.

We are closer, but not close enough, to technology compatibility. A better working relationship between DSS information technology team and its OPM counterparts has better enabled OPM's e–QIP security to mesh with the DOD IT system to facilitate overall clearance processes. As Mr. Johnson has mentioned, we are still in the process of adapting 100 percent to e–QIP and we hope to do that by the end of the year or even sooner.

DSS completed a very brutal zero-based review of its infrastructure funding requirements. This is a bedrock prerequisite toward establishing order in any budgetary household. We can also report progress toward meeting the requirements of IRTPA. DOD, including DISCO, is meeting IRTPA's requirements that call for 80 percent of the adjudications to be completed within an average of 30 days.

And we are strengthening our industrial security program. This remains a challenge to us, though. There are almost 12,000 cleared contractor facilities across the country. There are more than 25,000 information systems approved to process classified information, and DSS has a field workforce of less than 300. We have to balance resources against inspection and accreditation requirements, and it is clear when we do so that DSS must adopt a risk management approach to execute its industrial oversight role.

Another challenge is automation. DSS maintains IT systems upon which the defense community depends. New and changing requirements are taxing those systems. We are continuing to evaluate the best solution to our IT system requirements.

DSS infrastructure is another challenge. The personnel security industry function was transferred from DSS to OPM—the inspection function was transferred to OPM in February 2005. We at DOD planned inadequately to support the DSS infrastructure that remained in DOD after that transfer. DSS retained the responsibility to oversee OPM funding and financial reconciliation. We failed to recognize the magnitude of the cost of that oversight. That failure caused accounts for the so-called shortfalls for 2007–2008, sir. DSS has continued to work closely with the DOD comptroller to identify these funding challenges and to resolve them.

Finally, DSS's overarching challenge is to manage expectations. We must convey, and we have failed to do so so far, but we must convey to the rest of government and to the defense industrial contractor base a realistic sense of what DSS, its current budget and size, can be expected to support.

We are assessing the personnel security program from end to end. We will come up with concrete changes necessary to overhaul and streamline the program. We are committed to working with OMB, the Office of the Director of National Intelligence, and the interagency to bring about a new personnel security process for the government.

The Department's senior leadership is committed to correcting systemic problems. We realize necessary changes will take time. We will be providing progress reports on both our short-term and long-term efforts to fix DSS and on our efforts to fix the overall security clearance process.

Mr. Chairman, I want to conclude by thanking Members and staff for your support. You have helped us through a tough year. We pledge to you our best efforts and we are now available to answer any questions you may have.

Senator AKAKA [presiding]. Thank you very much for your testimony. Ms. Dillaman.

TESTIMONY OF KATHY L. DILLAMAN,[1] ASSOCIATE DIRECTOR, FEDERAL INVESTIGATIVE SERVICES DIVISION, U.S. OFFICE OF PERSONNEL MANAGEMENT

Ms. DILLAMAN. Mr. Chairman, Senator Voinovich, it is my privilege to testify today on behalf of the Office of Personnel Management and update you on our progress.

In his June 2005 Executive Order, President Bush directed that "agency functions relating to determining eligibility for access to classified national security information shall be appropriately uniform, centralized, efficient, effective, timely, and reciprocal." OPM Director Linda Springer takes that direction very seriously and has

[1] The prepared statement of Ms. Dillaman with an attachment appears in the Appendix on page 55.

included in OPM's Strategic and Operational Plan specific goals to ensure that we accomplish these expectations.

As you know, OPM provides background investigations to over 100 Federal agencies to assist them in making security clearance or suitability determinations on civilian as well as military and contractor personnel. Our automated processing system and vast network of field investigators handle an extremely high volume of cases. This year we will conduct over 1.7 million new requests.

Mr. Chairman, as you may recall, when the joint OMB–OPM Performance Improvement Plan was provided to your Subcommittee in November 2005, it addressed the critical areas of the overall security clearance process. As an attachment to my prepared testimony today, I have included a chart which outlines that process, the responsible agencies, and the timeliness goals that we have established for each step.[1]

Since developing that plan, we have made significant progress in improving overall timeliness and reducing the inventory of delayed cases, and we are continuing to work aggressively to resolve any issues that are hindering timely completion of background investigations. Our processing system tracks every step—from the time the subject completes and provides the necessary data and forms, to the date the agency makes the adjudication action, providing full transparency for the timeliness of each subject's clearance.

The first step addressed to improve overall timeliness is the timely and accurate submission of the subject's information for investigation. The expanded use of e–QIP has improved timeliness and has lowered the rate of submissions that OPM has to reject because they contain incomplete or inconsistent information. The use of the form has increased substantially to over 70 percent of all submissions this fiscal year to date, and in March 2007, submissions for initial clearances through e–QIP took 14 days. This is an improvement from the 35 to 55 days reported in November 2005. The rejection rate is currently 9 percent and we believe that that can be reduced to the 5 percent goal through expanded use of e–QIP.

We continue to make good progress in reducing the amount of time it takes to complete the investigations for initial clearances. Eighty percent of the over 137,000 initial clearance investigations that were requested in the first quarter of fiscal year 2007 are complete and they averaged 78 days in process, well below the 90-day standard set in the Intelligence Reform Act. In fact, almost 28,000 of these investigations were completed in less than 45 calendar days.

In addition, we significantly reduced the inventory of both initial and reinvestigations that were previously delayed in process. This fiscal year, on average, we are closing 13,000 more investigations each month—national security investigations—than we are opening, which means we are effectively reducing and eliminating that overage portion of our inventory. Continued performance at this level meets the statutory goals for applications for initial security clearances and will result in the timely completions of reinvestigations, as well, by October 1, 2007, as planned.

[1] The chart submitted by Ms. Dillaman appears in the Appendix on page 62.

The improvement in timeliness can be attributed in part to our increased staffing and productivity of our field agents. Currently, we have over 9,200 employees and contractors devoted to the background investigations program. In addition, we continue to work aggressively with national, State, and local record providers to improve their timeliness in providing information critical to the process. And while improving the timeliness of investigations, we continue to be vigilant about maintaining or improving the quality of the investigations we complete.

For adjudication, during the second quarter of fiscal year 2006, agencies averaged 78 days to adjudicate their investigations, with only 9 percent of those reported done within the 30-day standard of the Act. During the first quarter of fiscal year 2007, 80 percent of the over 128,000 adjudications reported to OPM were completed in an average of 33 days, which includes mail and handling time between OPM and the adjudicating agency.

We continue to work with agencies to improve the time it takes to deliver completed investigations, which includes the development of an imaging system that will allow us to electronically transmit completed investigations to those adjudication facilities. We are currently piloting that electronic transmission with nine agencies and we expect to be in a full production mode by October of this year. Next year, in 2008, the imaging system will be used to migrate from our current hard-copy file system, pending file system, to a virtual file system which will, in effect, make this process from beginning to end electronic and paperless.

We are pleased with the improvements that have been made, but we recognize that there is still much work to be done. We will continue to work with OMB and the clearance-granting agencies in order to meet the requirements Congress and the President have set on this critical issue.

This concludes my remarks and I would be happy to answer any questions you have.

Senator AKAKA. Thank you very much for your testimony, Ms. Dillaman. Now we will hear from Mr. Stewart.

TESTIMONY OF DEREK B. STEWART,[1] DIRECTOR, DEFENSE CAPABILITIES AND MANAGEMENT, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. STEWART. Good morning, Mr. Chairman, Senator Voinovich. Thank you for the invitation to come back again to yet the fourth hearing on personnel security clearances. We really do at the GAO appreciate your commitment to this issue. As you know, and I have testified all three times before that this is a very serious issue, critical to the national security of this country, and we mean that sincerely. So we appreciate your commitment to this issue.

Today, I will highlight the results of our September report that looked at clearances for industry personnel. Mr. Chairman, as you know, and Senator Voinovich, as you know, industry personnel have screamed the loudest about the problems with security clearances, because if they can't get their folks cleared, they can't do the work of the government and there is a cost involved in that for all

[1] The prepared statement of Mr. Stewart appears in the Appendix on page 63.

taxpayers. So this report focuses on Top Secret clearances for industry personnel. We looked at the timeliness and the quality of DOD and OPM's process to grant these clearances for industry personnel.

Mr. Chairman, I will tell you right up front that the results of our study are disturbing. I will address the timeliness issue first and then I will talk about quality.

We reviewed over 2,000 cases of industry personnel who were granted Top Secret eligibility in January and February of last year, and I want to emphasize that these cases are a year old. We looked at them last year, and at that time, OMB was and OPM was about 3 months into the reform effort. So I just want to make sure we have that reference.

Our analyses showed that the process took an average of 446 days, or about 15 months, for first-time clearances, an average of 545 days, or about 18 months, to update existing clearances, and an average of 111 days for the application submission phase of the process. Now, I would note that OMB's goal at that time was 14 days. The average time was 111 days.

Major factors contributing to these delays are an inexperienced investigative workforce, rejecting applications multiple times, not fully using technology, and in some cases requiring the manual entry of data, and multiple levels of application reviews. Now, those last three factors that I mentioned, that is the multiple rejection of applications, not fully using technology, and the multiple levels of reviews, those are critical factors and I just want to point out that the February report that was provided to Congress by the Security Clearance Oversight Group did not fully account for those factors, and I will come back to that point later.

Regarding quality, we found that OPM provided incomplete investigative reports to DOD and DOD used these incomplete cases to grant Top Secret clearance eligibility. Specifically, we randomly sampled 50 cases out of the over 2,000 cases I referred to earlier to determine the completeness of documentation. We found that almost all, 47 out of 50 cases, 94 percent, were missing key documentation required by Federal standards.

For example, of the 13 areas required to be addressed, we found that 44 out of 50 cases, 88 percent, were missing documentation for at least two and as many as six areas of the 13, and these cases managed to make their way from OPM to DOD despite OPM's quality control procedures. Now, we understand that the procedures have since been replaced with different procedures.

Also, 27 of the 50 cases that OPM sent to DOD contained 36 unresolved issues that were mostly related to financial matters, foreign influence, and personal conduct. Now, in such cases where there are unresolved issues, the DOD adjudicators should have requested OPM to provide additional information or at a minimum documented that additional information was needed. Neither of these things happened in these cases.

Mr. Chairman, the record will show that we expressed concern about the quality of the process when this Subcommittee had its second hearing in November 2005. Today, given the results of our study, we remain even more concerned about the quality of the process. There has been a lot of talk today about timeliness, but what does it profit us to do it fast and not get it right? So we are very concerned about the quality of the process, as well.

This concludes my prepared remarks. I will be happy to respond to questions.

Senator AKAKA. Thank you very much, Mr. Stewart. I appreciate all of your testimonies. We will now begin with questions.

Mr. Johnson, the President's Executive Order 13381 that gave OMB responsibility for defining roles and requirements for security clearances is set to expire. What changes will take place upon this order expiring?

Mr. JOHNSON. Well, it was set to expire. It was a 1-year Executive Order. It called for a time frame for OMB to be responsible. It was to end last June or July. We extended it for another year to keep us in charge. My guess is we are going to extend it another year. We have had thoughts about the responsibility for the oversight of the overall effort, leadership of the overall effort ought to pass to the Director of National Intelligence. They have some questions about that. Right now, it will continue to be OMB. I think we are doing a good job of moving it forward and will continue to be responsible for doing that.

The long-term responsibility still has to be determined. Right now, we are just taking it a year at a time.

Senator AKAKA. Thank you. Mr. Andrews, the Defense Security Service has consistently underestimated the number of investigations it plans to submit to OPM for the year. This makes it difficult for OPM to get enough staff to get through those investigations. My question to you is why does DSS continue to underestimate the number of clearances?

Mr. ANDREWS. That is a good question, Mr. Chairman. Estimating the clearance requests from over 12,000 contractors is based on a data call from about 400 of these contractors on a sampling basis each year, and so the very method of sampling has proven unsatisfactory. Also, too, Mr. Chairman, OPM faces a challenge in that the clearance request from the rest of the Department of Defense, not the contractors but from the Department of Defense, from the uniformed military services, do not pass through DSS and so Kathy Dillaman has to cope with requirements coming directly into OPM from Army, Navy, Air Force, and DSS has no picture of that flow, either. So it is a tough sampling process and we are working on it and we are going to need industry's help, sir. I don't know if Ms. Watson wants to comment more on that, but she can add details later.

Senator AKAKA. Yes, I would like further comment on what you are thinking about doing or what you are doing to fix this problem.

Ms. WATSON. Good morning. We have recognized that——

Senator AKAKA. Will you state your name?

Ms. WATSON. My name is Kathy Watson, and I am the Director of Defense Security Service. Good morning. The Department has recognized that its inability to properly predict its requirements for clearances is a problem not just for the Department, but for OPM. We recognized that a year ago, but DSS does not have the capability or the resources in house to actually help the Department predict those requirements. We recognized that last summer and we put forward in our budget request money to properly staff an office that would give us that capability.

I have obtained money and funding to staff that office beginning in fiscal year 2008 and we are now in the process of hiring for that office. I have money to hire 20 people so that we can get our arms around the requirements process at the Department. Right now, each different department and agency is essentially acting on its own. There is no overall methodology at the Department. We realize we need to fix that.

Senator AKAKA. Mr. Andrews.

Mr. ANDREWS. Let me add, Mr. Chairman, that we are talking about some gross numbers. The constituency for security clearances across the U.S. Government, the intelligence communities have about 3 percent of those clearance requests or requirements. The Department of Defense has 80 percent, so that gives you an idea of the relative magnitude of how important it is. And industry—this is of government clearances, so that will give you an idea of the challenge we face and Ms. Watson deals with daily.

Senator AKAKA. Ms. Dillaman, the Intelligence Reform and Terrorism Protection Act required that by December 2006, 80 percent of all investigations take no more than 90 days. By December 2009, it should be less than 60 days. Are you going to meet this goal?

Ms. DILLAMAN. Sir, we are certainly looking at what it is going to take to meet this goal. I think everyone recognizes that timely investigations cannot be at the cost of a good quality investigation. And because we rely on the voluntary cooperation of sources across the government and across this country, it is possible to overly compress the amount of time to the point where we are not getting the information we need to have a good quality investigation.

Certainly through staffing, use of technology, research into alternative record systems and methods of obtaining information, we can continue to pare it down. But a lot will depend on just how much innovation we can bring to this process between now and the 2009 goals.

Clearly, sir, we were capable of, in the first quarter, producing 28,000 investigations in less than 45 days. But that meant that the information for those investigations and those sources were readily available. That is not always the case.

Senator AKAKA. Thank you. Mr. Stewart.

Mr. STEWART. Yes, sir, Mr. Chairman.

Senator AKAKA. GAO has said that OPM inacurately reports, or fudges information relating to clearance investigations, leaving out a significant amount of time. What aren't they counting and why should they be counting it?

Mr. STEWART. Thank you for the question, Mr. Chairman. I hope GAO didn't use the word "fudge." That is not a GAO term.

No, it is exactly right, sir. The Security Clearance Oversight Group report to Congress in February points out in their report they are not counting all of the up-front time, the handoff time and the up-front time. The 111 days that I mentioned on average during the application submission phase, that is really the part that is not getting counted.

When OPM says we are processing clearances in 75 days or 60 days or whatever, I am not sure that those statistics include all of the time from the time that the security officer submitted the application to DOD, to DISCO, and then DOD looked at the application and may have sent it back to the security officer. Then they resubmitted. Then DOD sends it to OPM. OPM looks at it and it may find something wrong with it and it sends it back to DOD. DOD then sends it back. All of that time is not being counted. But the poor contractor, the industry person, is sitting out there waiting for his clearance and does not understand that all of this back-and-forth is going on and then the statistics show that once OPM finally scheduled it for an investigation, it took us X-number of days.

So we are concerned. We would like to see the up-front time counted in those statistics. The law says the time that it takes to do the investigative phase. Well, we consider all of that the investigative phase. Once it leaves the contractor, security officer, it is with the Federal Government. It is with DOD and then DOD sends it to OPM. That time should be counted, and as far as we know, it is not.

Senator AKAKA. Thank you very much.

Mr. JOHNSON. Mr. Chairman.

Senator AKAKA. Yes.

Mr. JOHNSON. Could I make a comment on a couple of questions you asked Mr. Stewart and Ms. Dillaman?

Senator AKAKA. Yes.

Mr. JOHNSON. Is that appropriate?

Senator AKAKA. Yes, since we are on the question.

Mr. JOHNSON. OK. On the comment by GAO, I want to point out and emphasize they don't have any current knowledge of what is going on in the security clearance process. Their information is 16 months old, when we began this reform effort. So what they are disturbed about is what we had, what the situation was at the beginning of the process 16 months ago. Nobody is claiming that we are where we want to be, but we welcome GAO to come in and take another sampling of what Ms. Dillaman does and Mr. Andrews does, to come in and take current samples of clearances and let us look at current information, not 16-month-old information.

GAO talked about their concern about the quality. I didn't hear any references to any quality measures that they were looking at or specific data that alarmed them or gave them cause for concern about the quality of the investigation work being done by OPM. They are not trying to present to you anything that wasn't what it is, but I want to emphasize that is really old information, before 16 months of effort was entered into to reform that performance and to improve that performance.

Senator AKAKA. Thank you.

Mr. JOHNSON. Thank you.

Mr. STEWART. Mr. Chairman, may I just very quickly——

Senator AKAKA. Yes, Mr. Stewart.

Mr. STEWART. Mr. Johnson is absolutely right. Most of our data is based on cases that were adjudicated in January and February of last year, as I mentioned in my oral statement, and a lot has changed in a year. However, I am holding up OMB's report to Congress that was submitted several months ago, in February, and this report says OMB has not addressed reinvestigations. OMB also has not included in its timeliness statistics the time of the handoff of applications to the investigative agency, handoff of investigation files to the adjudicative agency, return files to the investigative agency for further information. That is the part I am talking about. As these files are returned for further information, as they are handed off, as they go back and forth, the contractor is sitting there waiting for its clearance and all of this is going on.

So this should be captured in OPM statistics about how long it takes. It is erroneous to say it is taking us—we are doing everything—80 percent of everything that we are doing, we are doing it in less than 90 days.

Mr. JOHNSON. Mr. Chairman, there is nothing erroneous in that report, nothing. Not one utterance in that report is erroneous. We say what is in there. We are very specific about what is in there. We are very specific about what is not in there. And we are very specific in our discussion about our 2007 goals, objectives, self-imposed goals, is to develop end-to-end accountability for this process. There is not one erroneous piece of information or contention in that report.

Mr. STEWART. Mr. Chairman, if you are not capturing all the time in the investigative phase, which includes the application submission part—that is all the front-end part—then these statistics should be viewed with some skepticism.

Mr. JOHNSON. That report is very clear about what is there and what is not there and I personally resent the contention by GAO that is an erroneous report to Congress.

Senator AKAKA. Thank you.

Ms. DILLAMAN. If I may, sir, included in that report in February, there is also another chart that clearly shows we do measure those segments.[1] Obviously, we can't be responsible for the timeliness of the investigation until we receive a request. However, we do have full transparency from the time the subject completes his or her document until it is handed back to the adjudicating agency. The chart shows agency-by-agency the average number of days that the front-end process, that handoff, took, and yes, that has to be added to the investigation time.

In my testimony, I stated that the goal was to reduce that to 14 days. Anecdotally, we have evidence where it took much longer than the 111 days Mr. Stewart referenced. We have gotten agencies focused on timely submissions. E–QIP submissions are taking 14 days. Paper copy, 30 days, and that 30 days will reduce to 14 when we have full e–QIP submission. Nothing is being left out. We have full accountability from the time the person fires the starting pistol until we get it to investigate. That includes my piece, which is doing the investigation, a handoff, yes, but also timeliness then through adjudication.

Senator VOINOVICH. Ms. Dillaman, OPM has desiganted a category in the clearance process "closed pending." When a case is designated "closed pending," does the clock stop or is the time included when calculating the average case completion times as required by the Intelligence Reform bill? If so, I would be interested

[1] The chart submitted by Ms. Dillaman appears in the Appendix on page 62.

in understanding why OPM believes this is an accurate method of calculating the time it takes to complete an investigation.

Ms. DILLAMAN. Yes, sir. No, sir, it does not stop when we close it pending. Closed pending is an internal action within OPM to measure when the labor I need to provide has been provided. I may still be waiting on a third party. All of the data in our February report, all of our data which measures success under the Act is to "closed complete," final, which includes obtaining all third-party information.

Senator VOINOVICH. You don't take it off the clock if you put it in the closed pending file?

Ms. DILLAMAN. No, sir, only internally. Nothing that we are publishing now stops the clock at closed pending.

Senator VOINOVICH. As a result of the Subcommittee's oversight, a strategic plan was developed to monitor progress. Mr. Johnson, you indicated that you want to update that plan. Is that correct?

Mr. JOHNSON. You mean my opening remarks?

Senator VOINOVICH. Yes. One of the things that we did, and I felt real good about it, in fact, I bragged about it, is the fact that OPM, GAO, OPM and the Defense Department got together and developed a strategic plan, looking at the whole picture. Mr. Johnson, you have now had time to monitor what is wrong with the process and what is right. I am asking if you intend to update the plan?

Mr. JOHNSON. We have—our strategy on reforming this was to take the process that exists today, very manual, the same handoffs, and try to do the same work that we do now but do it better, and we thought that taking the process as is, doing it better, could get us to our December 2006 timeliness goals. We did for adjudication and we did for investigation, which was specifically called out by the Intel bill. The biggest issue is the end-to-end, from the very beginning to the very end, which was not a focus of the Intel bill but it needs to be and so we are changing our way of thinking about this to that end-to-end perspective.

We have all come to the conclusion that the only way we can get to the December 2009 goals of, I think it is 40 days for the investigation and 20 days for the adjudication, is we have to completely rethink the way we do this. We can't just do what we are doing now better. We have to do it differently. So what we need to do is there is a vision. DIA has a vision. The Director of National Intelligence has a vision. It has been shared in general terms with the leadership of this oversight group. What we need to do, and we will be able to do so within the next couple of months, is to come to you and say here is the way we envision this process working 2 years from now.

Senator VOINOVICH. Let me just say this. I am really concerned, because I don't believe that you are going to get it done by the time that you leave. I really don't. Senator Akaka, I have spent a significant amount of time on this issue. We need to have a pretty doggone good plan of what it is going to take to get the job done——

Mr. JOHNSON. Right.

Senator VOINOVICH [continuing]. Because when you leave, I would like to be able to take the next Administration and say, here is where we are at. Here are the things that need to be done. How are you going about doing them? I don't know about Senator

Akaka, but I would like to bring those people in that are going to be working on this immediately so we don't lose any time on the clearance reform process.

Mr. JOHNSON. Right. You will have that. What you have now, we committed to you in December—I mean, in February, this recent February, what our goals are and what we are going to work on this year, in 2007. One of those is a plan for the future, the new system, the new way of end-to-end, more automated, more use of commercial databases, more custom investigations and so forth. We will have a general picture to present to you, share with you within the next couple of months and we will keep you as current on that as you want to be and we will have by the end of 2008 a real clear knowledge of the validity, the likely validity of that and where that is going to be, and it may not be completely installed and the way we are doing our business then, but it will be really clear what the new, improved way of granting and determining security clearances ought to be. And so you will have that.

Senator VOINOVICH. I would like to have it. The individuals we are going to be hearing from on the second panel have been critical of OPM's dependency on imaging data, such as fingerprint cards, in automating the process. The second panel will testify that imaging does not equal automation because it does not allow for the image to be read for data extraction. They have many concerns.

It is important that we listen to industry to get their ideas on how we can do this better.

For example, I am really impressed with the improved rejection rate of initial applications because of e–QIP. It means somebody is talking and saying, hey, how can we come up with new technology to improve the process.

E–QIP is making a big difference. That is wonderful. There is less frustration with the agencies.

By working with industry, we are going to get this done. We are going to get this thing off the high-risk list, you hear me? Now, everybody says it can't be done, but by God, it is going to get done and we are all going to work together to do it.

Mr. JOHNSON. Well, this can be done. Nobody on this side of the table thinks this is impossible. No, this will be done.

Senator AKAKA. I agree with Senator Voinovich. We have 2 minutes before the vote is called on the floor. I am going to call a recess at this time. We will be back and we will continue to discuss these issues.

The Subcommittee is in recess.

[Recess.]

Senator AKAKA. This hearing will come to order.

I want to welcome Kathy Watson to the table.

I would like to say that before we recessed, there were some remarks that were made by Senator Voinovich and I want you to know he was right on target about what we are here to do. We are here to flesh out what we think needs to be changed and corrected and begin to put together a plan that we hope will work. That is what we are all here to do.

So let me begin by asking a question of Ms. Dillaman. OPM's investigations are almost entirely paper-based. Even when you get an electronic application, you print it out and you file it. All of that paper is then shipped back and forth to investigators and agencies with companies like FedEx. This seems like a waste of time and money. Why isn't OPM storing and sending documents electronically?

Ms. DILLAMAN. We are, sir. That is exactly the process we are going through now. Imaging our case papers and working in an entirely electronic mode is what is on the plate for this year. By the end of this fiscal year, all of our files will be imaged files. Next fiscal year, all the work in process will be imaged.

We reach out, sir, to hundreds of different types of sources and often the information they provide is delivered to us in paper form because that is how it is stored in those repositories, Federal, State, and local. We will then convert all of that to imaged documents, totally eliminating the paper, both for the pending investigations and for the completed investigations.

Senator AKAKA. This is a concern. Aren't we risking the privacy of a lot of sensitive personnel information when we let it out of the hands of the Federal employees and contractors?

Ms. DILLAMAN. Oh, absolutely, sir. We take every reasonable precaution to safeguard that sensitive information.

Senator AKAKA. Ms. Dillaman, your largest contractor, the U.S. Investigation Service, works for other government agencies, too, like Customs and Border Patrol. USIS completes a lot of those investigations faster by using their own computer software and processes. Why can't OPM do investigations as fast as its own contractor?

Ms. DILLAMAN. Sir, I don't believe that the computer system alone is the reason why investigations for some agencies can be done quicker. A lot of that has to do with volume, predictability of the location of those investigations, and the resources that contractor chooses to apply to those contractors.

Senator AKAKA. Is there any reason to think that those investigations are inferior to an OPM investigation?

Ms. DILLAMAN. I would have no basis to judge that, sir.

Senator AKAKA. Mr. Johnson, would OMB ever consider allowing DSS to use someone other than OPM to investigate their clearances?

Mr. JOHNSON. I would want to know why.

Senator AKAKA. You have been working with DSS and the question was whether you would consider allowing someone other than OPM to investigate.

Mr. JOHNSON. If that request came to me, I would ask, what is the definition of success here? What is the goal? What is the timeliness goal, the quality goal, the cost goal? What is the performance you are getting from OPM now relative to that goal and what do you believe you will get from an alternative source of investigative work? And understand what the risks of making a change are versus the benefits and then make a good decision. Our goal is to do the right thing for the Federal Government and for the taxpayers and if the right thing is to do it differently, we will seriously consider that.

Senator AKAKA. Well, let me ask a follow-up with Ms. Watson for any comment on what was just said. Do you think that you would want more options?

Ms. WATSON. DSS has been considering running a pilot program to see if there are alternative service providers for investigations so we can do a comparison on cost of investigation, the timeliness, and the quality, but we are restricted this year from doing that by reapportionment language we received from OMB.

Senator AKAKA. As I understand it, it could be that there is a problem in spending funds——

Ms. WATSON. Yes.

Senator AKAKA [continuing]. For any pilot projects that would use anyone other than OPM to investigate——

Ms. WATSON. Yes.

Senator AKAKA [continuing]. Clearances, and you are saying that that is correct?

Ms. WATSON. Yes.

Senator AKAKA. That the funding is a problem?

Ms. WATSON. Yes.

Senator AKAKA. Mr. Andrews, I understand that the computer program used by DSS, JPAS, has problems. Some would call it unreliable and on the verge of collapse. Can upgrades fix JPAS or does it need to be replaced?

Mr. ANDREWS. I think it needs to be replaced, sir.

Senator AKAKA. How long have you had that system?

Mr. ANDREWS. I don't have any idea, sir. Ms. Dillaman, do you know?

Ms. WATSON. DSS actually inherited that system from the Air Force. It was designed to do much less than we are asking it to do today. It has been upgraded by DSS for the last several years, although I don't recall the date that DSS assumed responsibility for the system. It has been upgraded numerous times to meet current requirements, and I can tell you that we aren't meeting current requirements with the upgrades we have, but we are now in a position where if we continue to upgrade it, we think it could kill the system.

Mr. ANDREWS. On a micro-sense, Senator, my perception is that if we put more money into JPAS, we are throwing good money after bad.

Senator AKAKA. Thank you. Ms. Dillaman, why isn't OPM counting the time that Mr. Stewart says should be?

Ms. DILLAMAN. We are, sir. All time is accounted for in our statistics. Again, sir, though, I can only be responsible for an investigation from the time I receive it until the time I complete it. But we can, however, track the time it takes to get to us and the time after the investigation is completed by our organization. Those statistics are provided and continue to be provided accurately and consistently and it is broken down by agency so that we can identify where those delays are.

Senator AKAKA. Thank you. Senator Voinovich.

Senator VOINOVICH. Yes. Getting back to JPAS, in your testimony, Mr. Andrews, you recommend the system be migrated to Defense Information System for Security (DISS), and discussed the high cost of migration. In light of your current budget shortfalls, how are you going to pay for it?

Mr. ANDREWS. We are working on it, sir. The short answer is that we are working with the DOD Comptroller to do just that. We are still in negotiation inside the Pentagon for that.

Senator VOINOVICH. You say that system is collapsing and you are going to go and get it done. Mr. Johnson said that the Defense Department has the money it needs. It is a question of allocating those resources to DISS. Is that the case, or don't you have the money? Ms. Watson, do you want to comment? All I want to know is are you going to have the money that you need to get the job done?

Mr. ANDREWS. As it stands right now, no, sir. Ms. Watson can fill in.

Ms. WATSON. No, sir, I don't have the money to do what I need now. I have enough money right now to sustain our current systems. JPAS is only one of five systems that we use to support the personnel security clearance process in the Department. DSS is responsible for the other four systems, as well.

To give you an idea of the cost just to sustain JPAS, just to keep it running costs me $10 million a year. My IT budget this year is $20 million. Ten million of that is going to just keeping one part of the system alive. There is not enough money left to upgrade the other systems, to keep them running, and to build a new system.

We have spent many hours working this issue with the Comptroller's office in the Department of Defense. We are continuing to scope the budgetary requirements. But I do not yet have funding that I need.

Senator VOINOVICH. So you are saying that the Defense Department isn't allocating resources that they have to your operation, or is it because you haven't had enough money made available to you in the appropriation process or request from the Office of Management and Budget?

Ms. WATSON. I don't have enough money made available to me. Part of that was because DSS probably did not request enough. We have in the past years. In the last year, it has not been funded. Whether or not the Department has that money and is not allocating it to me, I do not know the answer to that.

Senator VOINOVICH. Well, it sounds to me like button, button, who has got the button?

Ms. WATSON. Yes.

Senator VOINOVICH. Where are the buttons, Mr. Johnson? Is the money going to be there?

Mr. JOHNSON. DOD, as an entity, has all the money it needs to address the opportunities at DSS. They are talking about finding $10 million, $15 million, which is not even a rounding error at DOD.

DOD does not need more total money to fix security clearances.

Senator VOINOVICH. How is OMB going to work with DOD to help with the funding issues?

Mr. JOHNSON. We are going to help them—if they want to move money around within DOD, we will help them do that.

Senator VOINOVICH. Next week, I am meeting with Gordon England. I am going to find out whether he is going to reallocate the money. It seems to me it is incumbent on you to lean on these agencies to say they need to budget enough money to improve the security clearance process. Can I count on you to do that?

Mr. JOHNSON. You can count on me to deliver that message and communicate from Mr. England on down how important it is, but I can't make them reallocate that money.

Senator VOINOVICH. Senator Akaka, you are on the Armed Services Committee. I think you have a little clout there. Maybe the two of us will get Mr. England and get a commitment out of him that the money is going to be forthcoming.

Senator AKAKA. Well, there is no question the money is needed, so we will have to work on that.

Mr. JOHNSON. One of the questions you asked me, Senator Voinovich, was funding for general operations, continuous operations of DSS this year, was that assured, and I think your answer, Ms. Dillamon, is yes. The money that they are talking about not having is the money to change the way we do business and to upgrade or replace JPAS, is that correct?

Senator VOINOVICH. You haven't taken—I didn't swear you in.

[Laughter.]

Go ahead, Ms. Watson.

Ms. WATSON. Sir, right now, I am $25 million short for the rest of this fiscal year. There is a reprogramming action and I believe it made it to the Hill yesterday or the day before. It has the support of the Comptroller in DOD, it has the support of OMB, and now we are just waiting for Hill action. I anticipate that it will be acted upon favorably, but I don't have the answer to that yet. But that money will simply just sustain what I have through the end of this fiscal year. It is not to upgrade anything.

Senator VOINOVICH. Ms. Watson, how much money do you need?

Ms. WATSON. Twenty-five million will get me through this year. That is it. Yes, I need plus money for next year. We are working with the DOD Comptroller on what we actually need for next year. We do have an increase in our budget, but it is not enough and they understand that now. We are working through that issue.

And in terms of out years, 2009 and beyond, we are working that through the POM process. We know that we need approximately $200 million at a minimum to fund the next system, DISS. It is not inexpensive to do this work. And, in fact, if we are fully funded now, we can't deploy that new system until probably fiscal year 2010 or 2011.

Senator VOINOVICH. Well, I think that we are going to have to get together more often than hearings on this, Senator Akaka.

Ms. WATSON. And I want to get it done. I have the team assembled to do the work. I just need the money to do it.

Senator VOINOVICH. Our staff is very impressed with the management team. I agree with Mr. Andrews, your observation where you have a good management team. They are really impressed with the team that you have. So we are going to work with you real close to see if we can't make sure you get your money.

Ms. WATSON. Thank you. I will take all the help I can get.

Senator VOINOVICH. Yes. In all of the process of improving this, have any of you brought in the private sector to get their opinion about what they think needs to be done and how they can help or what their recommendations are? Mr. Johnson.

Mr. JOHNSON. With an eye towards how do we do it differently, how do we do it more like the private sector does? But they have a different challenge. We have a more complicated security clearance challenge than Wall Street firms and so forth. But nevertheless, sir, there are lessons to be learned, and yes, there has been a lot of conversation between Eric Boswell and John Fitzpatrick at the Office of the Director of National Intelligence. DOD has had a lot of conversations with outside firms, as well, about alternative ways of doing this. And so there will be a lot of consultation with outside firms, not only suppliers of and that will continue.

Senator VOINOVICH. You put together a strategic plan for security clearances. What input have you received? We are going to have a second panel here. What input have you or the Department of Defense or even Ms. Dillaman, in your operation, gotten from the private sector looking at the system and getting their thoughts on how they think that you can improve the system?

Mr. ANDREWS. Senator Voinovich, let me sort of drop down one level of granularity from Mr. Johnson. ODNI, Eric Boswell, the ambassador who was responsible for security for Mike McConnell, and I are meeting tomorrow under Mr. Johnson's sponsorship to put together a team that will come up with the new plan, in other words, not just fixing DSS, the present thing. We are working on very short internal time lines. I don't want to say what the time lines are because you will probably drop back one day and want a report on that, but let me say that one of your people on the panel following, Tim Sample, is going to be representing industry's input into that tiger team to work on the new process. So, yes, sir, we are.

Senator VOINOVICH. So you are going to bring him in and get his input?

Mr. ANDREWS. We have and we will.

Senator VOINOVICH. OK. Ms. Watson.

Ms. WATSON. On the IT side of the house, we knew we need to bring industry in to assist us in designing the new system. There is an acquisition management framework that we need to work through in the Department and that will allow us to get outside assistance. We talked to industry, in fact, some of our industry partners earlier this week, about their willingness to get involved in this process and assist us and our desire to take the assistance. To be honest with you, our team has been focused on the last 4 months just getting enough money to stay alive this year instead of doing outreach on what we can do with the new systems, and we know we need to change our focus and we will change that once we have some money.

Senator VOINOVICH. I will mention again that when I was mayor and when I was governor, I didn't use a lot of consultants. I don't know what the rules are in terms of ethics but it seems to me that if our friends that deal with the Department are concerned about security clearance, they ought to do some pro bono work to help out.

It is amazing what the private sector can do. It seems to me that the private sector could be very helpful in moving this along. If you can do it, you ought to take advantage of them.

Thank you, Senator Akaka.

Senator AKAKA. Thank you, Senator Voinovich.

Just to follow up on a response that you gave, Ms. Watson. You said that you were $25 million short when the question was asked about how much you needed. Since you are $25 million short now, how much do you need?

Ms. WATSON. We have done an assessment of what we need for next year to sustain ourselves versus what we need to improve ourselves. The difference is substantial. It is about $80 million. We are working to prove our case in the Department that we need that additional $80 million so that we can begin to make improvements.

Senator AKAKA. Thank you. Mr. Johnson, under the Intelligence Reform bill, agencies are supposed to allow for reciprocal security clearances from other agencies. This isn't happening at all agencies. Can you tell me why that is or what is the problem? Also, is OMB tracking the number of security clearances that must be redone?

Mr. JOHNSON. We are not where we need to be on the whole issue of reciprocity. One of the things we have come to realize is there is reciprocity in terms of granting a security clearance. There is also reciprocity with regards to determining suitability for employment. So if I want to hire somebody from DOD, there are two issues. Does their security clearance pass to me, do I reciprocate and accept the security clearance? Yes, but I still might want to do some additional investigation to determine the real suitability of that person for working at OMB, or whatever the agency is.

So the intelligence bill talks about security clearance reciprocity. There is also the issue of suitability reciprocity. We are trying to reconcile those, get those brought together so that it is the same issue, the same additional investigation or not that would have to be done, the determination to be the same. We are not where we want to be on that. But the general feeling is that in terms of reciprocity with regards to security clearances, that is not perfect, but it is better than it used to be and it is a pretty high level.

When we have looked at—we have the ability at OPM to look at when somebody requests a security clearance, background investigation be done, do they already have a security clearance? What is the incidence of that? Ms. Dillaman, do you know? Can you talk to that?

Ms. DILLAMAN. I can't address how often it happens, but I do know that we have an automatic stopper in the system that would keep an agency from reinvestigating someone who has a current, valid investigation on file.

Senator AKAKA. Mr. Johnson, I was asking about the number of security clearances that must be redone. Can you tell me how many clearances have been redone?

Mr. JOHNSON. I don't know, but I would bet it is next to none.

Senator AKAKA. Mr. Stewart, the GAO reported last September that more needs to be done by the OMB to fix the clearance process. Which part of the chain is the biggest problem, OMB, OPM, or DSS?

Mr. STEWART. Thank you for that question, Mr. Chairman. As you know, DOD's personnel security clearance program is on the high-risk list, so we have focused on DOD. I am encouraged by much of what I have heard here today from Mr. Andrews and others. But part of the problem that remains, and one problem that will have to be fixed, and I really want to emphasize this, we must fix this problem of DOD not knowing what its workload projections are, because that is one of the reasons we put them on the high-risk list and they are not coming off the list until they have a better way of projecting their workload.

Last year, Ms. Dillaman testified that DOD exceeded its workload goals by 59 percent. OMB's plan says that agencies will be within 5 percent of their workload projections. Today, I don't know where DOD is, but I would bet that they are not within 5 percent of the workload. So that is a big problem for us as we see it and that part has to be fixed.

The other part of this deals with technology, and you and Senator Voinovich have touched on pieces of this. We have not done an investigation of JPAS and PIPS, which is OPM's system, and the other systems out there, but we would love to have the Subcommittee to ask us to do that job because we feel that part of the fix to this problem goes to the technology that is in play right now.

You mentioned, Mr. Chairman, that USIS has systems in place that they use for other customers like NRO and other agencies that appear to be doing things faster. GAO would love to look at those systems. We have IT people in house, experts. We have the resources ready to go to do that job if you want us to do it.

So those two areas, I would say, DOD's workload projections and then the whole technological piece of this process, are where we think we really need to focus.

Senator AKAKA. Well, I want to thank you so much and thank this panel very much for your responses to our questions.

Mr. STEWART. Mr. Chairman, may I say one other thing?

Senator AKAKA. Mr. Stewart.

Mr. STEWART. I thought I was going to get a question and I didn't, but I just want to say this to you and Senator Voinovich. Mr. Johnson mentioned that it is likely that OMB will continue as the lead on this situation for the Federal Government, but at some point, this may go to the ODNI, the intelligence community, and if that happens, that will take GAO out of the picture. We have significant challenges working with the intelligence community. Comptroller General Walker has been meeting with Senator Rockefeller on the Senate Intelligence Committee. He has met with Congressman Reyes, Chairman of the House Intelligence Committee, to try to make a dent in this issue. So I just wanted to let the Subcommittee know today that if at some point this issue goes to the intelligence community, GAO will cease to have access to many of the records we will need to assist Congress in doing its work.

Mr. ANDREWS. Mr. Chairman, I hesitate to speak for my highers in the intelligence community, but I will tell you that neither the ODNI nor the USDI and the Department of Defense are casting any covetous eyes toward taking over Mr. Johnson's responsibility.

[Laughter.]

Mr. STEWART. Thank you, Mr. Chairman.

Senator AKAKA. Yes. Before concluding this panel, I want to mention that I have a bill, S. 82, that reaffirms this condition.

Mr. STEWART. Thank you for that, Mr. Chairman. We appreciate that.

Senator AKAKA. Again, I want to thank you very much and again repeat that Senator Voinovich and I are committed to looking at the problems we are facing and we are looking into all of the government's high-risk areas to see what we can do together to even come to improve it and do it better. We may also try to save money doing it. But this is a good part of the process, and again, I want to thank you. We are trying to fix whatever needs to be fixed, and we can only do that with your help. We continue to look forward to working with you on this.

I want to thank this first panel and encourage you to stay, if you can, to hear our second panel of witnesses. So thank you very much, and may I call up the second panel, please.

As Chairman of this Subcommittee, I would like to welcome our second panel, Timothy Sample, President of the Intelligence and National Security Alliance, and Doug Wagoner, Chief Operating Officer of Sentrillion, representing the Information Technology Association of America.

At this point in time, I am going to call for a recess of about 15 minutes. This Subcommittee is in recess.

[Recess.]

Senator AKAKA. The hearing will be in order.

It is the custom of this Subcommittee to swear in all witnesses, so I ask you to please stand, raise your right hand, and repeat after me.

Do you solemnly swear that the testimony you are about to give this Subcommittee is the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. SAMPLE. I do.

Mr. WAGONER. I do.

Senator AKAKA. Thank you. Let the record note the witnesses responded in the affirmative.

At this time, I welcome both of you, Mr. Sample and Mr. Wagoner, and ask for your testimony, Mr. Sample please proceed.

TESTIMONY OF TIMOTHY R. SAMPLE,[1] PRESIDENT, INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

Mr. SAMPLE. Thank you, Mr. Chairman. I am honored to be with you this morning to discuss this vitally important issue.

Mr. Chairman, I am the President of the Intelligence and National Security Alliance (INSA), which is a nonprofit, nonpartisan, professional association that focuses on intelligence and national security policy and practices. I wanted to mention that INSA's Counsel on Security and Counterintelligence is in the process of completing a white paper on today's subject, which I will be happy to forward to the Subcommittee once completed.

With regard to evaluating the progress in security clearance reform, I am skeptical about the data presented in the first panel, in part because there is no end-to-end process of evaluation, thus making valid, unbiased, empirical data hard to derive. The key, Mr. Chairman, is to significantly transform the process, not to update it.

[1] The prepared statement of Mr. Sample appears in the Appendix on page 85.

In response to the obstacles for success, I strongly agree with the Security Clearance Reform Coalition, of which INSA is a part, and with Doug Wagoner's testimony, including, I imagine, his oral testimony he will give in a minute. But in doing so, I also note that by instituting these changes alone, we end up with a more efficient but still very flawed system that never addresses the root cause of these problems, a culture steeped in risk avoidance. Saying this is not a criticism of security officers. It is a recognition of an overall approach.

Today, the personnel security process that we utilize is not that different from when it was implemented over 60 years ago. This process relies primarily on a front-end labor-intensive investigation with a periodic reinvestigation. But by focusing on government efforts on initial investigations, which we are now emphasizing in the attempt to decrease backlog, we are creating significant security risks as the backlog in periodic reinvestigations remain at a lower priority.

Let us remember that the most damaging spy cases of the past 15 years have been committed by those who have had access to classified information for decades, not those who just walked in the door. Ames, Hanssen, and Montes all worked under the same system we are evaluating today and worked for years before beginning to spy against the United States.

A second outcome of a risk avoidance culture is our inability to get the right people in the right job when we need them. Consider for a moment that under our current system, we likely would not hire the first and second generation Americans who were so critical in breaking Japanese codes in World War II or building the atomic bomb.

As Senator Voinovich stated, the impact on industry supporting government is also substantial. Private sector contractors have a difficult time filling positions the government requests. The government security requirements and the acquisition process have created a competitive marketplace to hire personnel based on whether he or she has a clearance, driving up salaries, bonuses, and costs. Ultimately, industry passes those costs on to you and me.

And society has changed enough over the past 60 years in a way that makes field investigations less effective than they once were. Although some pieces of valuable information can be discovered during field investigation, our society has changed to the point that in most cases, more information can be derived from available databases than from asking your neighbor whether or not you live within your means.

Mr. Chairman, the security community's risk avoidance culture is based on a threat posture, a society, and a pace of life that are well in our past. We attempt to avoid risk in a desire to achieve unachievable goals of absolute security and in the process we are now creating vulnerabilities in which others can capitalize.

We propose moving from a risk avoidance security culture to one based on risk management, as many companies around the world have done, recognizing that risk cannot be avoided but must be managed by putting in place mechanisms that would mitigate this risk through a robust ability to detect issues on a day-to-day real-time basis.

For example, a risk mitigation process could look to the financial sector. First, many companies that deal with the most sensitive insider information are cleared by an automated process of record checks, in some cases within 2 weeks, with a rigid monitored compliance structure to catch malfeasants.

Another example comes from the credit card industry. When I withdraw money from an ATM, the credit card company has a number of continuous safeguards to ensure that the card is legitimate, that I am the legitimate card holder, including by constantly evaluating my purchase habits and notifying me if something out of the ordinary transpires.

Mr. Chairman, there is no reason that the government could not adopt similar processes for granting and monitoring security clearances. In such a system, a clearance, once granted at a certain level for a certain job, would establish a security score, if you will, much like a credit score. That would be assigned to an individual for his lifetime and would be continuously monitored and adjusted based on a continuing assessment of the evaluation process.

The elements of such a system would include a fully automated government-wide application system, including electronic fingerprinting; a centralized automated investigation that would perform significantly robust database checks, more than we do today; an automated adjudication system that would take this applicant's score and compare it with the acceptable level of vulnerability for the specific job for which the individual has applied, potentially allowing granting some clearances through an automated process; an end-to-end case management system to ensure efficiency and effectiveness; an automated continuous evaluation system that would run in the background and would adjust the individual's score on a near-real-time basis, raising concerns when warranted; a system of aperiodic investigations that would be triggered randomly or from a continuous evaluation process; and a robust government-wide counterintelligence process.

Mr. Chairman, let me stress that this is not a proposal for a cost saving measure, although I do believe that substantial savings could be recognized over time. But we cannot do security on the cheap.

In addition, such a new system is achievable based on existing commercial technology models. Indeed, technology never has been the issue. It has been a matter of recognition and resolve.

And Mr. Chairman, if I could, let me mention from today's panel, I do have a little bit of concern about Mr. Johnson's statement that as they look to the future, they would look at a research and development project, and in those terms for the government, that usually suggests a time line that far exceeds what I think we can accomplish here and normally involves heavy reliance on manipulating legacy systems, which is something I think we need to get away from. Technology has far surpassed our legacy systems of today.

Heretofore, government leaders have relegated security to an administrative function. Only recently have they begun to understand the significant impact of today's process and the bureaucracy that supports it. There is a growing realization that today's process does not adequately meet today's threats, let alone those in the future.

Therefore, I implore the Subcommittee to consider the larger picture and support significant but necessary changes that have been offered. Thank you, Mr. Chairman.

Senator AKAKA. Thank you very much. Mr. Wagoner.

TESTIMONY OF DOUG WAGONER,[1] CHIEF OPERATING OFFICER, SENTRILLION, ON BEHALF OF THE INFORMATION TECHNOLOGY ASSOCIATION OF AMERICA

Mr. WAGONER. Good morning, Mr. Chairman and Senator Voinovich. My name is Doug Wagoner. I am the Chief Operating Officer of Sentrillion. I am speaking to you again today as a member of the Information Technology Association of America (ITAA) and would like to thank you for this opportunity for your continued commitment to reforming the clearance process.

Since 2003, ITAA has led the Security Clearance Reform Coalition of 10 trade associations to bring industry's recommendations to the clearance process. Several of our previous recommendations were adopted as part of the 2004 Intelligence Reform Act, which we talked about earlier this morning.

Industry continues to face significant problems with the clearance process that challenges our ability to meet national and homeland security missions. Delays in processing persist because of government's slow adoption of technology, agencies having their own requirements for clearances, and funding mechanisms that prevent investment in technology to save time and money.

Industry's recommendations can be summed up as this: One application, one investigation, one adjudication to create one clearance. Our detailed recommendations to achieve this are found in the addendum to my testimony. I would like to highlight one recommendation from each section.

The application: Industry believes that the single biggest impact to the entire clearance process would be the adoption of a 100 percent digital application. There are three parts to the application, the 30-page SF–86, a signed release form, and fingerprints. Industry applicants for DOD now use the electronic questionnaire, e–QIP, for the SF–86, but the other components of the application are not collected electronically.

Fingerprints are still collected and submitted using paper and ink cards. This baffles industry, since the Armed Services recruits, DHS's certification of port workers, and much of local law enforcement all use digital fingerprints. Industry has offered to provide the technology to submit digital fingerprints, but this offer was declined because databases are incapable of accepting the digital prints. The problem is that the fingerprint cards must be mailed and then later connected with the electronic application, creating significant opportunity for lost, delayed, or mismatched cards, which delays the start of the investigation.

The lack of a 100 percent digital application is causing a new serious problem, known as out-of-sync applications. Out of sync applications are e–QIP applications that appear to have been submitted successfully to the JPAS system, but in reality these out-of-sync applications are lost in the digital ether. We estimate over 2,000 in-

[1] The prepared statement of Mr. Wagoner appears in the Appendix on page 93.

dustry applications are out of sync and potentially tens of thousand more from DOD service members. Out-of-sync applications are only discovered by a diligent security officer who follows up on a delayed application.

Industry would like to recognize the efforts of the new Director of Defense Security Service Kathy Watson for identifying these and other problems and making suggested improvements to JPAS, but as we heard this morning, we are disappointed by the lack of funding and prioritization from the Department.

An easy solution to implement would be for OPM to enforce their 2-year-old published requirement for government-wide use of e–QIP. OPM continues to accept 25 to 40 percent of all applications in paper, with agencies like GSA sending 100 percent of their applications using paper. A complete digital application would start the investigation process in minutes, as opposed to days or weeks, and lead to greater automation of the rest of the process.

Investigation: OPM's Federal Investigative Services Division (FISD), is responsible for 90 percent of the investigations of all clearances granted. Here, too, the process needs technology to eliminate the tremendous amount of touch labor. For example, all files, even those submitted electronically, are printed out and placed in doctor office-style folders with colored tabs created for each applicant. It is industry's opinion that this paper shuffling between Boyers, Pennsylvania, and the field creates delays in clearance processing.

Industry recommends that government create an end-to-end data management process using e–QIP. The data collected here could then be electronically verified via commercial and government databases, such as credit histories and criminal records. This type of data is the linchpin to make billions of dollars of risk-based decisions in the financial and insurance industries. The DNI is currently studying the use of this type of data for investigations and we look forward to their findings.

All this data would go to adjudicators as an interoperable electronic file to assist in the speed and accuracy of the adjudication process, and this is going beyond imaging, which we have heard about this morning. Imaging is simply taking a picture of a piece of paper. What we want is to capture the data electronically and then move it around, manipulate it, analyze it, and really use the data as opposed to just taking a picture.

Adjudication: Adjudication can be improved through better definition of derogatory information in the course of the investigation. Currently, some derogatory information is not fully developed in the investigation, imposing long and unnecessary risk assessments on adjudicators. We still believe that adjudicators are a critical part of the process of evaluating trustworthiness, but intentionally leaving issues undeveloped or labeling applications as "closed pending" exacerbates the condition and makes it harder for adjudicators to accurately assess an applicant. Often, this case is sent back for reinvestigation, only to clog the backlog.

Reciprocity: Bill Leonard at the Information Security Oversight Office should be applauded for his efforts to bring about greater reciprocity throughout government. Frequently, his efforts are overcome by the intractibility of old habits. This is in spite of reciprocity requirements in the 2004 Intelligence Reform Act. Limited trust in other agencies' investigations or adjudicative abilities is at the heart of the reciprocity problem. Empowering OPM as the single investigative source for most clearances was the correct step towards establishing uniformity of the process. Other steps, like the CIA sharing unclassified clearance information to JPAS, are applauded as enhancing reciprocity. However, government-wide sharing is still limited. As the sole system of record for collateral clearances, all agencies need to use JPAS.

Budget: In conclusion, Congress must provide innovative and flexible budgetary authority to agencies to allow for needed technology and process improvements. FISD, for example, receives no funds but instead pays for their operations through agency customer fees. This pay-as-you-go system cannot budget for new time and cost-saving technology detailed in our recommendations.

Mr. Chairman, we hope that these recommendations provide options to improve our clearance process. We are ready to discuss all the recommendations in the addendum and look forward to working with you and the Subcommittee to bring about additional improvements to national security by improving our clearance process.

Senator AKAKA. Thank you very much, Mr. Wagoner. Now we will have a round of questions.

Mr. Wagoner, cleared workers have become a hot commodity for contractors. Want ads for a lot of jobs now say that you shouldn't even apply if you don't have a clearance already. I worry that contractors now may be more concerned with finding someone with a clearance than finding someone with the best skills for the job. Do you agree with this?

Mr. WAGONER. There is no doubt that we have customers to serve, we have contractual requirements that we must meet, and there is tremendous pressure placed upon the industry for the cleared personnel. At the end of the day, I can't imagine any contractor putting an unqualified person in a job just because they have a clearance. At the end of the day, that is going to come out in your performance. It is not good business.

But what you are seeing, as opposed to us putting unqualified people in the job, is us paying much more for these folks. As the COO of a company that does a lot of cleared work, I am stealing from my peers, they are stealing from me, and every single time the person makes a jump, they are jumping for 5, 10, 15 percent more salary. Someone alerted me today out in the hallway that there is a company that says if you were hired in the first quarter of this year, we are going to put your name in a hat—if you have a clearance—and if we pull your name, you are going to get a new BMW, not even an American car. So the pressure is great, but it is greater on the financial side of the business than our performance.

Senator AKAKA. Mr. Sample, apparently some agencies in the intelligence community can do background investigations faster than OPM. In your experience, how long does it take to get an intelligence clearance versus a DOD clearance?

Mr. SAMPLE. Mr. Chairman, thank you for that question. Obviously, part of that is position-dependent and job-dependent, but I think that there is a growing track record now, for example, it was mentioned this morning and I think mentioned earlier that the National Reconnaissance Office, for example, has instituted some significant technological advancements in their process as well as the ability to conduct their investigations in a much more robust fashion so that they have time lines that are down into, I believe, the 30 to 40-day requirements. That is not in all cases, clearly, but I think for a vast majority, that is true and I would be happy to come back to the Subcommittee with a much more firm time line.

Senator AKAKA. Why do you think that the intelligence clearance is faster? Are their standards lower or different than Defense's?

Mr. SAMPLE. I think it is because there are different standards for each different agency. I think that is part of it. But more importantly, I think an individual agency within the intelligence community has much better control and insight and the end of the overall process. They know when something is being held up. They know how to manage that. It is something that allows them to be more flexible, to be better responsive during the investigation, and consequently, they can move at a much faster pace.

Senator AKAKA. Mr. Wagoner, in your testimony, you refer to OPM's investigative database, PIPS, as antiquated and say that in the private sector, it would have been replaced as an out-of-date hindrance to efficiency. However, in a report last February to Congress, OPM praised the system as a model of speed, reliability, and security. Can you tell me why you don't share OPM's assessment of PIPS?

Mr. WAGONER. I think the best way to answer it is in my testimony when I noted that there are things that we all would like to add, be it moving data around, adding the digital fingerprint, adding a digital signature, and at the end of the day, the reason we can't implement those other technologies, which we use every day—you go to a supermarket, you have your digital signature. I mean, this is not super-advanced technology. The problem is that you can't bolt these kinds of advancements onto PIPS. It is just that antiquated.

As an ancillary note, I am not sure if they are true—we have heard stories of bringing people out of retirement to maintain PIPS because the languages that were used to build that are so old, the documentation was so poor, they brought folks back just to maintain it. So I cannot imagine how it could be the model for efficiency.

Senator AKAKA. Senator Voinovich.

Senator VOINOVICH. Were you here when the other witnesses were testifying?

Mr. WAGONER. Yes, sir, I was.

Senator VOINOVICH. OK. One of the questions I asked them is what input have they gotten from their customers in order to improve their system. I would like to know from you is what communication has your organizations had with OMB, OPM, and Defense?

Mr. SAMPLE. Thank you, Senator. INSA has had a continuing dialogue with government. A lot of our work actually has been through the coalition that Mr. Wagoner is here to represent today. Recently, however, we have had a significant amount of interaction with the Department of Defense, and I give them credit in saying that the Deputy Secretary has recognized that something significant needs to be changed if the Department of Defense is going to be able to manage their clearance process and their security process in the future and they had asked me to come in——

Senator VOINOVICH. You are talking about Gordon England now?

Mr. SAMPLE. Yes, sir.

Senator VOINOVICH. OK.

Mr. SAMPLE. And the new USDI, Jim Clapper, and also Bob Andrews, the witness from this morning, brought me in and asked me to really take a look at this and advise them as they start to structure what a new system might look like.

Consequently, I think that there has been some awakening within DOD. I am encouraged by it. As Mr. Andrews said, they are continuing to reach out and INSA will come together and support their needs as they go forward.

I also would add, and Mr. Andrews mentioned this, that there are now meetings between the DNI, DOD, and OMB to really look at what a future system that is much more like the one that I described in my opening statement might look like and whether or not that is achievable, and we will certainly support them in every aspect that they need.

Senator VOINOVICH. Mr. Wagoner.

Mr. WAGONER. While ITAA and the Security Clearance Coalition may differ with the progress that has been made, or maybe the solutions that need to be implemented, I can tell you that all——

Senator VOINOVICH. The coalition is made up of who again?

Mr. WAGONER. It is made up of the Aerospace Industries Association, Armed Forces Communication Electronics Association, NDIA, Professional Services Council, Mr. Sample's organization, INSA, Association of Old Crows, Contract Services Association, American Council of Engineering Companies, and there is one I may be missing.

Senator VOINOVICH. OK. We have it here in front of us.

Mr. WAGONER. OK.

Senator VOINOVICH. Yes. Good.

Mr. WAGONER. But I can tell you that all the witnesses this morning, and in addition DNI, have been very open. Any questions, they always take our calls. We have several meetings a year. They come to talk to our members to report on progress——

Senator VOINOVICH. Have you had meetings recently with them? It seems like from what Mr. Sample said that there seems to be a renewed interest at the Department of Defense——

Mr. WAGONER. I met with representatives from DNI's study group of clearances just last week, had a meeting with them personally. Ms. Dillaman has briefed our coalition on a regular basis, I would say at this point, on her progress.

Senator VOINOVICH. Who did you meet with at DNI?

Mr. WAGONER. It was Mr. Capps, representing Mr. Fitzgerald, who is working on the pilot project looking at data.

Senator VOINOVICH. What is your observation in terms of the sincerity of these folks?

Mr. WAGONER. I think it is very sincere. I think they want to make a difference. I think they understand the problem. I think they understand, to your point, sir, that there is an end customer that has a mission, a national security mission to complete. It is inter-government challenges, it is the budgetary challenge. We just can't seem to get to the goal line.

Senator VOINOVICH. Now, the JPAS system, Mr. Andrews says, is collapsing and that he recommends that the system be migrated to the Defense Information System for Security, DISS, and discussed high costs of migration. In light of DSS's current budget shortfalls, is it your opinion that they don't have the resources to get the job done?

Mr. WAGONER. Yes, sir. They do not have the resources to get the job done, nor—I am not familiar with that organization, DISS. I don't know how a simple transfer of an application is going to help. I do agree that engineering needs to start now on something new very close to what Mr. Sample's recommendations were, really looking at a new business process and an application to support that new business process.

Senator VOINOVICH. Do you think OMB, OPM, and DOD understands what has to be done?

Mr. SAMPLE. Senator, I believe certainly within DOD they understand that, or certainly they are starting to. I think Mr. Andrews understands that and he has been pushing for looking at a new system. In relation to DISS specifically, it is a system that has been in development. It has a significant budget. I am not convinced yet whether at the end of the day it is the right system, and I only say that because it is designed to meet the current processes, and if you go along the line of saying you need to change your business processes going forward on how you do this, then there is a likelihood that system may end up not being adequate for what you need.

Senator VOINOVICH. That is one of the questions that I would ask Gordon England. Are they really sure that transfer to DISS is the right technology solution.

Mr. SAMPLE. Yes, sir.

Mr. WAGONER. You do not want to automate a poor process.

Senator VOINOVICH. You heard a lot of the testimony this morning. I would be interested in your comments about it. Do you think there were some inaccuracies or exaggerations?

Mr. SAMPLE. Senator, I think my interpretation of this morning's panel is you had a group of people who, I believe, are trying to do a good job under the current system. I think that their goals and their guidelines thus far have been to make the system that they have better and respond to the backlog issue. I think that not all of them have gotten to the point of understanding that the process itself may be the problem, let alone the systems that are involved, and I think, as I said in my statement, I think there is an awakening there, but it is slow to come and it is the first time I know with my experience in the security arena, the first time I have seen this many high-level individuals in various agencies who are actually looking at this and understanding there is a problem and are willing to consider what, for government, are fairly dramatic changes.

Senator VOINOVICH. Mr. Wagoner, your comments?

Mr. WAGONER. Yes, sir. Mr. Stewart's recognition that—of course, it obviously was open for contention on the days—I am glad he brought that up, because industry has been frustrated by the numbers that we get out of OPM where they continue to say, well, we are doing better, the investigation is shorter, the adjudication is shorter. The problem is, we meet with our membership every month and we understand it is anecdotal evidence, but this is across many companies, across many associations. Generally speaking, we don't see it getting better for the Top Secret clearances. Maybe a few days, but we don't see the dramatic change that would be as evidenced in the February report from OPM. So I am glad Mr. Stewart raised that today and maybe everyone can get together on reconciliation of exactly when does the process start and when does it end and then we can get some good numbers and set some good metrics.

Mr. SAMPLE. Senator, if I could add, what is interesting is, and Mr. Wagoner just said that some of this is anecdotal, but ironically, from my time in the intelligence community, from my time in the House, and now from my time with INSA, I don't run into someone who has been in government and has had a security clearance who doesn't have some relatively dramatic story about their own personal interaction with the security clearance process and the delays involved.

Senator VOINOVICH. It is amazing to me that even though Congress has required improvements in the security clearance process, many agencies are not abiding by these mandates. At this stage of the game it is fair to say that the process is broken and has not been improved.

Mr. SAMPLE. No, sir, I don't believe it has. And one last comment is that I mentioned what I consider to be the risk avoidance nature of this culture right now. Mr. Chairman, you had asked about the PIPS system and one of the comments that was made earlier was how secure they say it is. Well, of course it is secure. It connects to nothing.

[Laughter.]

But if your goal is absolute security at the expense of getting the job done to support national security, then at what cost is your business process?

Senator VOINOVICH. I have run out of my time. Senator Akaka.

Senator AKAKA. Do you have further questions?

Senator VOINOVICH. I would like to stay in touch with both of your organizations. It would be nice, maybe, on a monthly basis as to how you think things are moving along. Are you able to provided input? As I mentioned to Mr. Johnson, I think that we are going to push them hard for this plan. I would like to, as soon as possible, get your reaction to the plan so that if there are major concerns that you have, that we can raise them in the beginning rather than getting on the track and just stay with it.

I really believe that, from what I can ascertain, that there is a real sense of—more of a sense of urgency. We have a golden opportunity to return this process. But if we don't stay on it on a very regular basis, it is not going to get finished.

The last thing is, how do you think Ms. Watson is doing?

Mr. SAMPLE. My experience with Kathy Watson has been tremendous. I think she is the right person for that job right now. The fact that they have taken the step of taking the "acting" away from her title will be tremendous. I think her management skills are shown in the leadership team she has put together and I think it is an issue at this point of giving her not only the trust, but the backing and support to allow her to get her job done.

Mr. WAGONER. I think she is phenomenal. I think we all need to support her and give her what she needs. I think she will make good use of it. She knows what needs to be done. She was prepared today. She is phenomenal, very open with industry and definitely wants to make a difference.

Mr. SAMPLE. Senator, one last comment about Ms. Watson is that fixing DSS and fixing the overall process are two different issues, and sometimes they get intertwined. The importance of fixing DSS, though, is regardless of how you come out with the overall process, even with the best improvements you can make, if you can't hand it off to a healthy DSS, then you have undercut your whole effort.

Senator VOINOVICH. Right. So DSS has to be in the position where they can send the information over to OPM and do it in as efficient a way as possible. When it comes back to DSS they need to be able to adjudicate it as quickly as possible. They are fundamental to the security clearance process.

Mr. WAGONER. And the other role they have is as the owners of JPAS, which should be the system that everyone uses for clearances. Giving her the funding to get that where it needs to be once we all agree on the new process would help all of government, not just DOD.

Senator VOINOVICH. Thank you, Mr. Chairman.

Senator AKAKA. Thank you very much. This has been a great discussion. Your testimonies were to the point, and again, I am repeating that this Subcommittee will continue to work on this issue. As Senator Voinovich said, we can't let it continue. You have been very helpful with your responses.

The reason that we are really going after this is our country has been speaking so much about national security and this process is so vital to our national security. When investigating this, I couldn't believe the information I was finding, and because of that, I couldn't just sit there and let it go. So Senator Voinovich and I, I want you to know, are going to stick with this, and as we pointed out, we are going to flesh out the problems and work on them, correct them, improve them, and also try to plan for the future.

As my friend, Senator Voinovich said, we can't wait for the next Administration. I am so glad that he also mentioned that we need your kind of help. As you said, Mr. Sample, we can't just change things, we have got to transform what is there and we need to do it in a manner where everybody wants to be a part of the process.

So I want to say thank you to our witnesses for discussing with us this critically important issue. We must continue to work to get DOD's clearance process off GAO's high-risk list. We have heard very valuable testimony today and I think it will be very useful as we move forward. I want to thank you also for your patience. Usually, we don't have as many recesses as we had today. I also want to thank my friend, Senator Voinovich, for being such a huge part of this hearing.

The hearing record will be open for a week for additional statements or questions from Members. With that, this hearing is adjourned.

[Whereupon, at 12:42 p.m., the Subcommittee was adjourned.]

APPENDIX

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

DEPUTY DIRECTOR
FOR MANAGEMENT

Statement of

The Honorable Clay Johnson III

before the

Subcommittee on Oversight of Government Management,
the Federal Workforce and the District of Columbia

of the

Committee on Homeland Security and Governmental Affairs

United States Senate

May 17, 2007

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

- For requests for initial security clearances from agencies served by OPM (90% of total clearances), 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, is 95 days (75 days for investigation and 20 days for adjudication).
- 80% of the initial clearance investigations performed by OPM, completed after October 1, 2006, averaged 103 days, while 80% of the adjudications by those agencies whose investigations are performed by OPM, completed and

recorded after October 1, 2006, averaged 18 days. The combined averages for investigative and adjudicative times averaged 121 days for 80% of those completed after October 1, 2006.

- ALL investigations completed by OPM after October 1, 2006 averaged 162 days, while ALL adjudications completed and reported by agencies whose investigations are done by OPM, averaged 41 days; so the total of the two averages is 203 days.

However, improving investigative timeliness and adjudicative timeliness for initial clearances does not mean we are most assuredly granting security clearances as quickly as desired.

- 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 determination within the agency, once the investigation and adjudication are complete.
- Some of the performance information I reference here is 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

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		
	Average Days	*392 days*	*347 days*
	Secret/Confidential		
	Average Days	*179 days*	*155 days*

Reinvestigations for Top Secret Completed	*Average Days*	*579 days*	*482 days*

The President designated The Office of Management and Budget (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 the 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 March 31, 2007, 81% of the 49,051 initial clearance investigations initiated by OPM during October 2006 have been completed. Average processing time for these is 77 days. Seventy-two percent of the 6,272 requests for Top Secret level investigations have been completed in an average of 101 days, and 82% of the 42,779 investigations for Secret/Confidential level have closed in an average of 74 days.
- For 45,676 initial clearance investigations that were completed and forwarded to agencies for adjudication in October 2006, 78% have been reported as adjudicated in an average of 19 days.
- DOD (92% of total adjudications) has reported adjudications on 79% of their investigations completed in an average of 19 days. Non-DOD agencies have reported adjudication on 71% of their investigations completed in an average of 26 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 346,005 initial investigations completed by OPM during the 1st and 2nd quarters of FY 07 averaged 103 days in process. The difference between the timeliness of these investigations versus those requested and completed after October 1, 2006 (77 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 162 days. The average initial security clearance investigation took 205 days in 2004, 188 days in 2005, and 176 days 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 April 2, 2007, that number was reduced to 49,691 investigations pending in process more than one year. Of these, OPM has completed all required basic coverage for over 26,000 that are now awaiting third-party records and/or a special subject interview to address issues developed during the investigation.
- For 164,428 initial adjudications completed and recorded during the first two quarters of FY 07, 80% averaged 18 days to process, while the average time for all was 41 days.
- DOD (89% of this activity) averaged 18 days for 80% of the 146,522 actions reported, and Non-DOD agencies averaged 19 days for 80% of the 17,906 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 two quarters of FY 07 averaged 257 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.

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.

Research & Development

I reiterate that just because investigative and adjudicative performance has improved, we are still not granting security clearances as quickly as desired. 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.

PERSEREC is also 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 are developing and institutionalizing 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.

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.

Conclusion

Ongoing efforts to improve the security clearance process are aggressive. We will not slow down until the efficiency and effectiveness of the security clearance process is as we desire it to be.

STATEMENT

OF

MR. ROBERT ANDREWS

DEPUTY UNDER SECRETARY OF DEFENSE
(COUNTERINTELLIGENCE AND SECURITY)

BEFORE
SUBCOMMITTEE ON OVERSIGHT OF GOVERNMENT MANAGEMENT, THE FEDERAL WORKFORCE, AND THE DISTRICT OF COLUMBIA
SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

HEARING
ON
EVALUATING PROGRESS AND IDENTIFYING OBSTACLES IN IMPROVING THE FEDERAL GOVERNMENT'S SECURITY CLEARANCE PROCESS

MAY 17, 2007

Introduction:

Good morning Mr. Chairman and members of the Committee. I am pleased to appear before you today.

I am Bob Andrews, Deputy Under Secretary of Defense for Counterintelligence and Security, under whose oversight the Defense Security Service (DSS) falls. I am joined by Ms. Kathleen M. Watson, Director of the Defense Security Service (DSS).

I appeared here one year ago to report on the budget crisis at DSS. That crisis led to the suspension of processing personnel security clearances for industry. DSS took this action because it did not have sufficient funds to pay the Office of Personnel Management (OPM) for investigations.

I can report that DSS corrected many of the root causes that led to last year's shutdown—namely internal housekeeping concerns like leadership challenges and a lack of standard operating procedures.

Are we satisfied with our progress to date? No, we are not. Much work remains to be done both at DSS and across the Department and interagency. We will need to work together to solve long-term, systemic problems that continue to plague DSS and the clearance system.

Let me start by addressing what we have accomplished since my last appearance before this Committee.

Successes:

Permanent Leadership Team. As I stated last year, the primary concern was a failure of leadership. DSS went through several directors over the past few years—all acting—and nine comptrollers in the last four years.

I am pleased to report that we have made tremendous progress in establishing a permanent leadership team for DSS. Kathleen M. Watson was named the director of DSS on February 19, 2007. She is the first permanent director at the agency in five years. Kathy assembled a core management team in her first few months on the job. This team is new, focused, and committed to the success of DSS.

Prior to her appointment, Kathy served as acting director for six months. I asked Kathy to provide an independent, unbiased look at DSS. That is, to identify what caused the fiscal train wreck of last year and more importantly, to prevent a recurrence.

Through the help of an acting Comptroller, we have gotten to "ground truth" at DSS. We are charting a path to recovery. The path is not an easy one and will require the support and commitment of the Department of Defense to ensure its success.

Let me briefly outline several of the solutions we have implemented.

- Close Working Relationship with OPM. The Defense Security Service (DSS) has reinvigorated its working relationship with OPM. Together, DSS and OPM are working to create a new process to better serve our customers.
- Surcharge Issue Resolved. As a result of OMB mediation, we have worked out our disagreement with OPM over the rates OPM charges DoD for investigations.

OPM agreed to refund DoD $7 million in FY 2006, and for FY 2007 OPM eliminated the surcharge. Now DoD pays the same rates as other Federal agencies.

- Information Technology Compatibility. A closer working relationship between the DSS Information Technology Team and OPM counterparts ensured that OPM's e-QIP security form is compatible with the DoD IT system to facilitate the overall clearance process.
- Stronger DoD-wide Coordination. We told you that we will establish a Clearance Oversight Office (COO) to act as the DoD conduit with OPM for requirements and support. In FY08, DSS will receive funding to establish this office. This office will work with the military services and defense agencies to identify, validate, prioritize and monitor all DoD-wide requirements for personnel security investigations.
- Financial Transparency. DSS made significant progress in getting its budgetary house in order:
    - DSS conducted a zero-based review of its infrastructure funding requirements and is working with DoD Comptroller to ensure these requirements are properly funded in the outyears.
    - DSS's resource management process identifies, vets, and prioritizes resources to assure proper distribution of funds.
    - DSS's corporate board makes financial decisions for the agency putting DSS in line with government best practices.

  - DSS's financial analysis system links program development to actual budget execution across the agency.
  - DSS contracts review process more accurately analyzes deliverables and burn rates to ensure all requirements are validated and accounted for.
  - DSS's financial standards measure mission accomplishment.
  - DSS is reviewing its program funding requirements and will work any funding issues on this with the DoD Comptroller.
- Compliance with the Intelligence Reform and Terrorism Prevention Act of 2004. DSS's Defense Industrial Security Clearance Office, also known as DISCO, processes requests for industrial personnel security clearances, requests industrial PSIs from OPM, and adjudicates security clearances for industry personnel under the National Industrial Security Program. DoD, including DISCO, is meeting the adjudicative timelines established in the Intelligence Reform and Terrorism Prevention Act of 2004, which requires 80 percent of adjudications to be completed in an average of 30 days.
- Strengthening our Industrial Security Program. DSS initiated an internal review to address new ways of doing business in the National Industrial Security Program. With almost 12,000 cleared contractor facilities across the country, more than 25,000 information systems approved to process classified information, and a field workforce of less than 300, DSS must adopt a risk management approach to execute its industrial security oversight role.

Remaining challenges:

DSS still has many challenges ahead. A major one is automation. DSS maintains IT systems upon which the defense security community depends. As with other information technology systems in the Department, new and changing requirements are taxing DSS's legacy systems. We are continuing to evaluate the best solution to our information system requirements. To that end, our new Defense Information System for Security (DISS) system will undergo the highly structured and disciplined Department's Major Automated Information System (MAIS) process, to ensure there is proper oversight and the best solution is obtained.

DSS infrastructure costs present another funding challenge. When the personnel security industry (PSI) function was transferred from DSS to the OPM in February 2005, there was insufficient planning for funding to support DSS infrastructure. Remaining in DoD, DSS retained the function, on behalf of DoD, to oversee the OPM billing and financial reconciliation process for PSIs for the entire Department. DoD, however, had no process to identify, validate, prioritize, fund, and monitor investigation requirements. The zero-based review of DSS' infrastructure funding requirements will form the basis of deliberations with Under Secretary of Defense (Comptroller) to ensure these requirements are properly funded in the outyears.

DSS has continued to work closely with the Under Secretary of Defense for Intelligence and the Under Secretary of Defense (Comptroller) to identify its funding challenges and to resolve them.

DSS has a challenge to manage expectations within the rest of government and within the defense industrial contractor base, to convey a realistic sense of what DSS—at its current size and budget—can be expected to support.

The Department as a whole is meeting the benchmarks in the Intelligence Reform and Terrorism Prevention Act.

Need for Real Change:

The Department is committed to working with Congress in its efforts to improve the personnel security process. The Office of the Under Secretary of Defense for Intelligence, the Office of the Deputy Under Secretary of Defense for Counterintelligence and Security, and the Defense Security Service Director, are assessing the personnel security program from end-to-end and proposing changes necessary to overhaul and streamline the program. We are committed to working with the interagency, to include the Office of Management and Budget and the Office of the Director of National Intelligence.

It is clear that the present process for personnel security investigations will not support our national needs in the coming years. It is a labor intensive process that is increasingly vulnerable to attack or exploitation by adversaries and expensive to maintain. DSS and the Department can only move forward with a commitment to overhaul the process from top to bottom to achieve desired timeliness and quality. We will propose changes in the near term and over the next several years. Some changes can be accomplished with revised policy, others if funding is received, and still others with strengthened relationships among agencies.

Conclusion:

The Department's senior leadership is committed to correcting systemic problems in the personnel security process, but we realize the necessary changes will take time.

We are prepared to meet with the Committee periodically to provide progress reports on both our short-term and long-term efforts to correct the problems identified.

Mr. Chairman, this concludes my prepared remarks. We are available to answer any questions you may have.

Statement of

Kathy L. Dillaman
Associate Director
Federal Investigative Services Division
Office of Personnel Management

before the

Subcommittee on Oversight of Government Management,
the Federal Workforce, and the District of Columbia
Committee on Homeland Security and Governmental Affairs
United States Senate

on

Evaluating Progress and Identifying Obstacles in Improving the Federal Government's Security Clearance Process

May 17, 2007

Mr. Chairman and Members of the Subcommittee, it is my privilege to testify today on behalf of the Office of Personnel Management (OPM) to provide you with an update of the progress that has been made to improve the timeliness of the security clearance process and reduce the backlog of background investigations.

In his Executive Order dated June 28, 2005, President George W. Bush directed that "agency functions relating to determining eligibility for access to classified national security information shall be appropriately uniform, centralized, efficient, effective, timely, and reciprocal." OPM Director Linda Springer takes that direction very seriously and has included in OPM's Strategic and Operational Plan specific goals to ensure we accomplish the expectations set by the President and by the Congress in the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA).

Background

OPM's mission is to ensure the Federal Government has an effective civilian workforce. To accomplish this mission, OPM provides background investigation products and services to agencies to assist them with making security clearance or suitability decisions on civilian, as well as military and contractor personnel. OPM conducts different levels of investigations for various types of positions in the Federal Government. The investigations range from the minimum level of investigation for positions that require a Confidential or Secret clearance, to extensive field investigations for those that require a Top Secret clearance.

At OPM, the division responsible for conducting background investigations is our Federal Investigative Services Division (FISD), headquartered in Boyers, Pennsylvania. This division supports over 100 Federal agencies and has security offices across the country and worldwide. Our automated processing systems and vast network of field investigators handle a high volume of cases. In fact, we expect we will have conducted over 1.7 million investigations by the end of this year.

As an attachment to my prepared testimony today, I have included a chart which further outlines the various steps in the security clearance process, from the initial request for a clearance through the investigations phase to the adjudications and clearance determination phase. Included in this chart is a column identifying the timeliness goals for each step which I will describe in more detail in my testimony.

Update on the investigation and security clearance process

Since 2005, OPM has had lead responsibility for about 90 percent of all personnel background investigations for the Federal Government. This percentage reached that level as a result of statutory authorization concerning transfer of Department of Defense (DoD) background work Our authorities in this area were formalized as a result of the President's Executive Order which led to operational designations from the Office of Management and Budget (OMB). We have been working closely with OMB, which has the lead for policy setting on this issue. We also are working very closely with the major clearance granting agencies to meet the timeliness requirements under IRTPA.

Mr. Chairman, as you may recall, when the joint OMB-OPM Performance Improvement Plan was provided to your subcommittee in November of 2005, it addressed four critical areas of the investigation and security clearance process: workload projections, timeliness and quality of agency submissions of investigations, investigations timeliness, and adjudications timeliness.

Since that time, I am happy to report that significant progress has been made in improving overall timeliness and reducing the inventory of cases, and we are continuing to work aggressively to resolve any issues that are hindering the background investigations process.

OPM's automated processing system, known as "PIPS", effectively tracks each step of the security clearance process -- from the time the subject provides the necessary data and forms, to the date the agency makes an adjudicative decision. This system provides full transparency for the timeliness of each subject's clearance. Additionally, each quarter we provide OMB and the clearance granting agencies a report on the progress that has been made to meet the four areas I just outlined in our plan goals. Let me elaborate on each of these four areas:

Workload projections: To staff the investigative program responsibly, we need agencies to work toward projecting their annual need within a margin of 5 percent. For Fiscal Year 2007, we are finding that agency submissions to OPM thus far have been less than originally predicted with respect to initial security clearance investigations. Overall, however, the total number of agency submissions for all types of investigations – both for clearances and for suitability decisions -- have increased.

Timeliness and quality of agency submissions of investigations: The first step in improving the timeliness of the investigation and security clearance process is timely and accurate submission of the subject's background information to OPM. The expanded use of the electronic Questionnaires for Investigations Processing (e-QIP) by submitting agencies has improved timeliness and has lowered the rate of submissions OPM rejects because they contain incomplete or inconsistent information. Overall use of the electronic form has increased substantially to 70 percent this fiscal year, with the Department of Transportation, Department of Commerce, and Department of Education currently meeting the goal of 100 percent e-QIP usage.

In March 2007, submissions for initial clearance investigations through e-QIP averaged 14 days while hardcopy submissions averaged 30 days. This is an improvement over the 35 to 55 calendar days reported in November 2005, with e-QIP submissions meeting the performance goal of all submissions within 14 days. In addition, the rejection rate is currently 9 percent, and we are confident this number can be reduced to the performance goal of less than 5 percent with the expanded use of e-QIP.

Investigations Timeliness: OPM continues to make significant progress in reducing the amount of time it takes to complete the investigations for initial security clearances. In April 2006, the timeliness for investigations used to support Top Secret clearances averaged 171 days, and investigations used to support Secret or Confidential clearances averaged 145 days. Looking at the initial clearance investigations received during the first quarter of FY 2007, 80 percent of the 137,925 initial clearance investigations received from October through December are now being closed with an average processing time of 78 days, so we are seeing significant improvement. In fact, 27,821 of these were closed in less than 45 days.

In addition, we have made tremendous progress in reducing the inventory of both initial and reinvestigations that were delayed in process. In October 2006, we had 385,695 pending national security initial and reinvestigations in process. As of April 28, 2007, the pending inventory of investigations received prior to FY 2007 was reduced by 74 percent to 100,869 that remain pending. Overall, we have been processing over 13,000 more investigations per month than we are receiving, rapidly reducing the over-aged portion of this inventory.

We believe these figures demonstrate that we not only have adequate capacity to handle new workloads, but that we have built sufficient capacity to maintain processing timeliness on initial clearance investigations while improving timeliness on reinvestigations. Continued performance at this level meets the statutory goal for applications for initial clearance investigations and we believe such performance will result in elimination of the reinvestigations backlog by October 1, 2007, as planned.

The improvement in timeliness can be attributed in part to our increased staffing and productivity by our field agents. Currently, we are maintaining a staff level of over 9,200 employees and contractors devoted to the background investigations program. In addition, we have worked aggressively with national, state, and local record repositories to improve their timeliness providing information critical to the process.

While improving the timeliness of investigations, we have been vigilant in maintaining the quality of our investigative products. We have developed additional internal quality control processes to ensure that the quality of completed investigations continues to meet the national investigative standards and the needs of the adjudication community. Overall, less than 1 percent of all completed investigations are returned to OPM from the adjudicating agencies for quality deficiencies.

We have also focused resources to improve the timeliness of required international coverage. We began deploying field agents overseas in August 2005, and at any given time, there are approximately 60 investigators working in over 71 locations around the world. We are also using State Department resources to assist with international coverage. Because of these efforts, we reduced the backlog of cases needing overseas coverage by more than 60 percent.

Adjudications Timeliness: During the second quarter of FY 2006, agencies averaged 78 days to adjudicate their investigations with 9 percent done within 30 days of completion of the investigation.

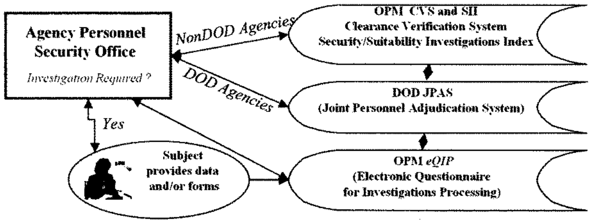
During the first quarter of FY 2007, agencies reported 127,905 adjudications to OPM. Of these, 80 percent were reported as adjudicated in an average of 33 days which includes up to 14 days in mail and handling time between OPM and the requesting agency. OPM continues to work with the agencies to improve the time it takes to deliver completed investigations and to report their adjudication actions. These efforts include the development of an imaging system to electronically transmit the completed investigations to the adjudications facility and linking an agency's in-house record system to OPM's data base for electronic updating of their actions. We are currently piloting electronic transmission with nine agencies, and expect production deployment in October 2007. In FY 2008, we expect that this imaging system will be used to migrate from hardcopy pending case files to a virtual case file system which will further streamline processing times within OPM and across Government.

Mr. Chairman, as I hope my testimony has shown, OPM is making significant progress to improve the overall timeliness of the security clearance process while ensuring we produce quality investigative work that will help agencies make decisions on whether an individual working for the Federal Government can be trusted if given access to national security information. While we are pleased with the improvements that have been made, we recognize that there is more work to be done. We will continue to work with OMB and the clearance granting agencies in order to meet the requirements Congress and the President have set on this critical issue.

This concludes my remarks. I would be happy to answer any questions the Subcommittee may have.

The Security Clearance Process

Step 1 – Subject selection and determination that a clearance is required



Agency Personnel Security Office

Investigation Required ?

NonDOD Agencies

DOD Agencies

Yes

Subject provides data and/or forms

OPM CVS and SII
Clearance Verification System
Security/Suitability Investigations Index

DOD JPAS
(Joint Personnel Adjudication System)

OPM *eQIP*
(Electronic Questionnaire
for Investigations Processing)

Request for Investigation Submitted to OPM Electronically and/or Hardcopy

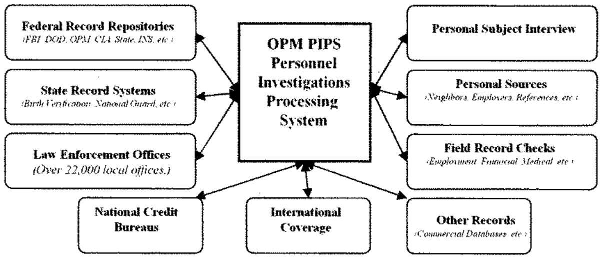
(SF 86 data, fingerprint chart, release)

•Annual investigation workload projections are within 5% of actual submissions

• Required investigations submitted for processing within 14 calendar days of subject completion of the SF 86 (hardcopy or eQIP)

• No more than 5% of all submissions rejected due to insufficient data/ information provided by subject or agency

Step 2 – Conduct Investigation



OPM PIPS
Personnel
Investigations
Processing
System

Federal Record Repositories
(FBI, DOD, OPM, CIA, State, INS, etc.)

State Record Systems
(Birth Verification, National Guard, etc.)

Law Enforcement Offices
(Over 22,000 local offices.)

National Credit Bureaus

International Coverage

Personal Subject Interview

Personal Sources
(Neighbors, Employers, References, etc.)

Field Record Checks
(Employment, Financial, Medical, etc.)

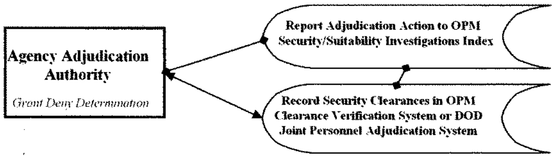
Other Records
(Commercial Databases, etc.)

<u>Investigations:</u>
• 80% of initial investigations completed within 90 days of receipt of all required forms/data

National Agency <u>Record Repositories:</u>
• 90% of all search requests (including file requests) completed within 30 calendar days

<u>International Coverage</u>
• 90% of all requests completed within 30 calendar days

Steps 3 and 4 – Adjudicate Investigation and Make Clearance Determination



Agency Adjudication Authority

Grant Deny Determination

Report Adjudication Action to OPM
Security/Suitability Investigations Index

Record Security Clearances in OPM
Clearance Verification System or DOD
Joint Personnel Adjudication System

• 80% of all investigations are adjudicated within 30 calendar days of the date the investigation was completed.

• Agencies report all adjudication actions to OPM within 30 days of the action taken.

United States 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

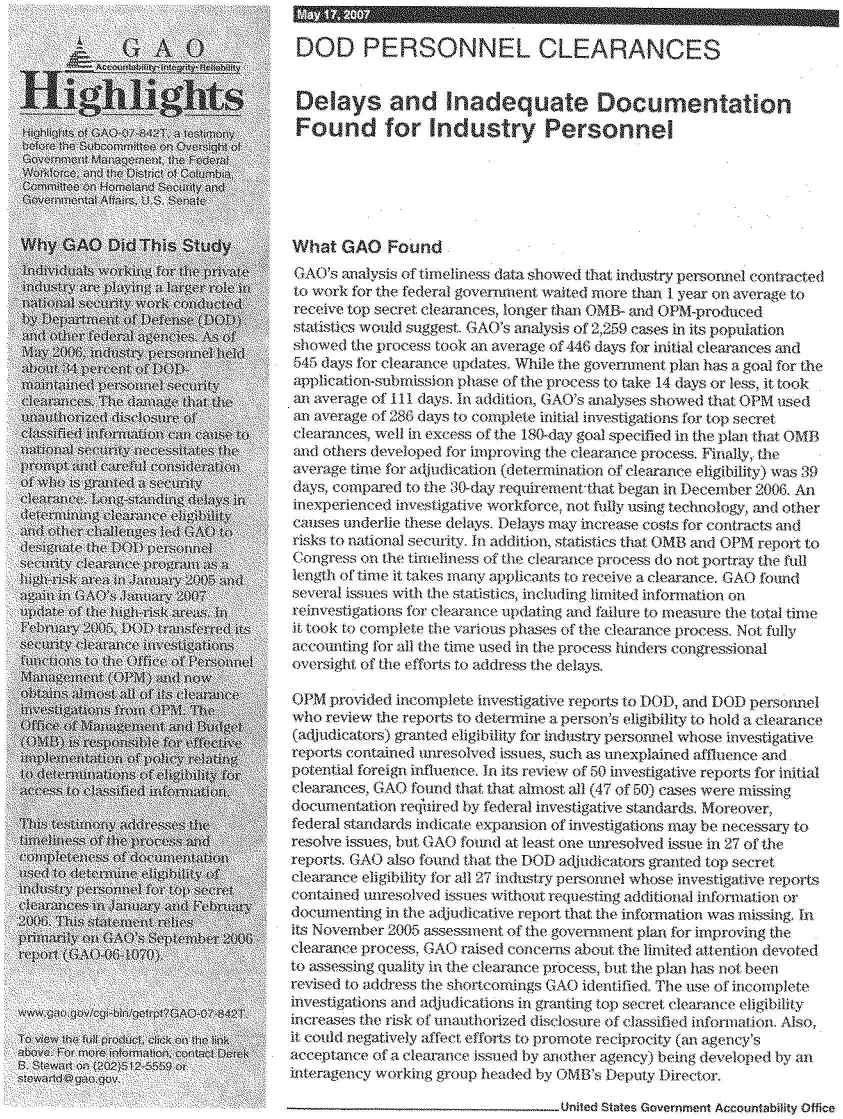
For Release on Delivery
Expected at 9:30 a.m. EDT
Thursday, May 17, 2007

DOD PERSONNEL CLEARANCES

Delays and Inadequate Documentation Found for Industry Personnel

Statement of Derek B. Stewart, Director
Defense Capabilities and Management

GAO
Accountability * Integrity * Reliability



GAO

Accountability·Integrity·Reliability

Highlights

Highlights of GAO-07-842T, a 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

Why GAO Did This Study

Individuals working for the private industry are playing a larger role in national security work conducted by Department of Defense (DOD) and other federal agencies. As of May 2006, industry personnel held about 34 percent of DOD-maintained personnel security clearances. The damage that the unauthorized disclosure of classified information can cause to national security necessitates the prompt and careful consideration of who is granted a security clearance. Long-standing delays in determining clearance eligibility and other challenges led GAO to designate the DOD personnel security clearance program as a high-risk area in January 2005 and again in GAO's January 2007 update of the high-risk areas. In February 2005, DOD transferred its security clearance investigations functions to the Office of Personnel Management (OPM) and now obtains almost all of its clearance investigations from OPM. The Office of Management and Budget (OMB) is responsible for effective implementation of policy relating to determinations of eligibility for access to classified information.

This testimony addresses the timeliness of the process and completeness of documentation used to determine eligibility of industry personnel for top secret clearances in January and February 2006. This statement relies primarily on GAO's September 2006 report (GAO-06-1070).

www.gao.gov/cgi-bin/getrpt?GAO-07-842T.

To view the full product, click on the link above. For more information, contact Derek B. Stewart on (202)512-5559 or stewartd@gao.gov.

May 17, 2007

DOD PERSONNEL CLEARANCES

Delays and Inadequate Documentation Found for Industry Personnel

What GAO Found

GAO's analysis of timeliness data showed that industry personnel contracted to work for the federal government waited more than 1 year on average to receive top secret clearances, longer than OMB- and OPM-produced statistics would suggest. GAO's analysis of 2,259 cases in its population showed the process took an average of 446 days for initial clearances and 545 days for clearance updates. While the government plan has a goal for the application-submission phase of the process to take 14 days or less, it took an average of 111 days. In addition, GAO's analyses showed that OPM used an average of 286 days to complete initial investigations for top secret clearances, well in excess of the 180-day goal specified in the plan that OMB and others developed for improving the clearance process. Finally, the average time for adjudication (determination of clearance eligibility) was 39 days, compared to the 30-day requirement that began in December 2006. An inexperienced investigative workforce, not fully using technology, and other causes underlie these delays. Delays may increase costs for contracts and risks to national security. In addition, statistics that OMB and OPM report to Congress on the timeliness of the clearance process do not portray the full length of time it takes many applicants to receive a clearance. GAO found several issues with the statistics, including limited information on reinvestigations for clearance updating and failure to measure the total time it took to complete the various phases of the clearance process. Not fully accounting for all the time used in the process hinders congressional oversight of the efforts to address the delays.

OPM provided incomplete investigative reports to DOD, and DOD personnel who review the reports to determine a person's eligibility to hold a clearance (adjudicators) granted eligibility for industry personnel whose investigative reports contained unresolved issues, such as unexplained affluence and potential foreign influence. In its review of 50 investigative reports for initial clearances, GAO found that that almost all (47 of 50) cases were missing documentation required by federal investigative standards. Moreover, federal standards indicate expansion of investigations may be necessary to resolve issues, but GAO found at least one unresolved issue in 27 of the reports. GAO also found that the DOD adjudicators granted top secret clearance eligibility for all 27 industry personnel whose investigative reports contained unresolved issues without requesting additional information or documenting in the adjudicative report that the information was missing. In its November 2005 assessment of the government plan for improving the clearance process, GAO raised concerns about the limited attention devoted to assessing quality in the clearance process, but the plan has not been revised to address the shortcomings GAO identified. The use of incomplete investigations and adjudications in granting top secret clearance eligibility increases the risk of unauthorized disclosure of classified information. Also, it could negatively affect efforts to promote reciprocity (an agency's acceptance of a clearance issued by another agency) being developed by an interagency working group headed by OMB's Deputy Director.

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss the Department of Defense's (DOD) personnel security clearance program and problems that continue to negatively affect that program. We have testified on clearance-related issues in three prior hearings that this Subcommittee has held since January 2005 when we first placed DOD's security clearance program on our list of high-risk government programs and operations.[1] To facilitate an understanding of our recent findings on private industry personnel who applied for top secret clearances,[2] I would like to first provide some information about the clearance process and events that have occurred since we placed DOD's program on our high-risk list.

DOD is responsible for about 2.5 million security clearances issued to servicemembers, DOD civilians, and industry personnel who work on contracts for DOD and 23 other federal agencies. Individuals working for the private industry are playing an increasingly larger role in national security work conducted by DOD and other federal agencies as a result of an increased awareness of threats to our national security stemming from the September 11, 2001, terrorist attacks and increased efforts over the past decade to privatize federal jobs. As of May 2006, industry personnel held about 34 percent of DOD-maintained personnel security clearances.

As with servicemembers and federal workers, industry personnel must obtain security clearances to gain access to classified information, which is categorized into three levels: top secret, secret, and confidential. The level of classification denotes the degree of protection required for

[1] GAO, *DOD Personnel Clearances: New Concerns Slow Processing of Clearances for Industry Personnel*, GAO-06-748T (Washington, D.C.: May 17, 2006); *DOD Personnel Clearances: Government Plan Addresses Some Long-standing Problems with DOD's Program, But Concerns Remain*, GAO-06-233T (Washington, D.C.: Nov. 9, 2005); and *DOD Personnel Clearances: Some Progress Has Been Made but Hurdles Remain to Overcome the Challenges That Led to GAO's High-Risk Designation*, GAO-05-842T (Washington, D.C.: June 28, 2005). Since January 2005, we have provided the Subcommittee with additional information in our answers to sets of questions for the records: GAO, *DOD Personnel Clearances: Questions and Answers for the Record Following the Second in a Series of Hearings on Fixing the Security Clearance Process*, GAO-06-693R (Washington, D.C.: June 14, 2006), and *Questions for the Record Related to DOD's Personnel Security Clearance Program and the Government Plan for Improving the Clearance Process*, GAO-06-323R (Washington, D.C.: Jan. 17, 2006).

[2] GAO, *DOD Personnel Clearances: Additional OMB Actions Are Needed to Improve the Security Clearance Process*, GAO-06-1070 (Washington, D.C.: Sept. 28, 2006).

information and the amount of damage that unauthorized disclosure could reasonably be expected to cause to national defense or foreign relations. For top secret information, the expected damage that unauthorized disclosure could reasonably be expected to cause is "exceptionally grave damage;" for secret information, it is "serious damage;" and for confidential information, it is "damage."[3]

DOD's Office of the Under Secretary of Defense for Intelligence (OUSD(I)) has overall responsibility for DOD clearances. Two offices are responsible for adjudication (eligibility determination to hold a clearance) for industry personnel. The Defense Industrial Security Clearance Office (DISCO) within OUSD(I) is responsible for adjudicating cases that contain only favorable information or minor issues regarding security concerns (e.g., some overseas travel by the individual). The Defense Office of Hearings and Appeals (DOHA) within the Defense Legal Agency is responsible for adjudicating cases that contain major security issues (e.g., an individual's unexplained affluence or criminal history), which could result in the denial of clearance eligibility.

Long-standing delays in determining clearance eligibility and other clearance challenges led us to designate DOD's personnel security clearance program as a high-risk area in January 2005 and continue that designation in the updated list of high-risk areas that we published in 2007.[4] In February 2005, DOD transferred its security clearance investigations functions to the Office of Personnel Management (OPM) and now obtains almost all of its clearance investigations from OPM, which conducts about 90 percent of all federal clearance investigations. Other recent significant events affecting DOD's clearance program have been the passage of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)[5] and the June 2005 issuance of Executive Order No. 13381,[6] Strengthening Processes Relating to Determining Eligibility for Access to Classified National Security Information. IRTPA included

[3] 5 C.F.R. § 1312.4, *Classification of National Security Information* (2006).

[4] GAO, *High-Risk Series: An Update*, GAO-05-207 (Washington, D.C.: January 2005), and *High-Risk Series: An Update*, GAO-07-310 (Washington, D.C.: January 2007).

[5] Pub. L. No. 108-458.

[6] The White House, Exec. Order No. 13381, (June 27, 2005). On June 29, 2006, the executive order was extended until July 1, 2007.

milestones for reducing the time to complete clearances, general specifications for a database on security clearances, and requirements for reciprocity of clearances (the acceptance of a clearance and access granted by another department, agency, or military service). Executive Order No. 13381 assigned the Office of Management and Budget (OMB) responsibility for the effective implementation of a uniform, efficient, effective, timely, and reciprocal policy related to determinations of personnel eligibility for access to classified information.

In June 2005, OMB's Deputy Director of Management was designated as the OMB official responsible for improving the process by which the government determines eligibility for access to classified national security information. One of OMB's efforts to improve the security clearance process involved taking a lead in preparing a November 2005 strategic plan to improve personnel security clearance processes governmentwide. In its February 2007 annual IRTPA-mandated report to Congress,[7] OMB noted additional improvements that had been made to the clearance process governmentwide. For example, OMB indicated that it had issued reciprocity standards, OPM had increased its investigative workforce to an estimated 9,367 total staff in efforts to reach an earlier goal of having 8,000 full-time staff, and agencies had dramatically increased the use of OPM's Electronic Questionnaires for Investigations Processing (eQIP) system to reduce the time required to get a clearance by 2 to 3 weeks. The report also identified several challenges associated with accessing records repositories.

In requesting our past work, you have expressed concern about the negative consequences of untimely, inadequate, or inconsistent investigations and adjudications. This testimony summarizes our earlier work that examined those issues and supplements other clearance-related reports that we have issued since originally placing DOD's personnel security clearance program on our high-risk list (see the list of Related GAO Products at the end of this statement). It addresses two questions: (1) How timely are the processes used to determine whether industry personnel are eligible for top secret clearances? and (2) How complete is the documentation of the processes used to determine whether industry personnel are eligible for top secret clearances?

[7] Office of Management and Budget, *Report of the Security Clearance Oversight Group Consistent with Title III of the Intelligence Reform and Terrorism Prevention Act of 2004* (February 2007).

This statement relies primarily on GAO's September 2006 report.[8] In conducting our prior work on these two key questions, we reviewed laws, executive orders, policies, and reports related to the timeliness and completeness of security clearance investigations and adjudications for industry personnel as well as servicemembers and civilian government employees. Those sources provided the criteria used for assessing timeliness and documentation completeness, and identified causes for and effects from delayed clearances and incomplete investigative and adjudicative reports. Additional insights about causes of and effects from delayed clearances and incomplete investigative and adjudicative reports were obtained from interviews with and documentary evidence from personnel associated with a variety of government offices: OUSD(I), DISCO, DOHA, other DOD adjudication facilities that make clearance determinations for servicemembers and DOD civilians; DOD's Defense Personnel Security Research Center; the Defense Security Service's Training Academy that offers adjudicator training; and OPM. Nongovernmental organizations supplying information on conditions, causes, and effects included officials representing two of OPM's investigations contractors and technology associations whose member organizations require clearances for their industry personnel. We also reviewed the February 2007 annual IRPTA-mandated report to Congress by the Security Clearance Oversight Group. For the timeliness question, our analyses of conditions included a review of computerized data abstracted from DOD's Joint Personnel Adjudication System (JPAS) and statistical reports on timeliness that OPM produced for DOD. The abstract was for the population of 1,685 industry personnel granted initial top secret clearances and 574 industry personnel granted top secret clearance updates by DISCO during January and February 2006. The clearance investigations for those 2,259 industry personnel were started at various times prior to the adjudications. While we found problems with the accuracy of some of the JPAS data, we determined they were sufficiently reliable for the purposes of our September 2006 report. DOD and OPM also supplied timeliness statistics for other periods, levels of clearances, types of personnel, and agencies to provide us with a broader context with which to interpret the timeliness statistics that we computed from the JPAS database abstract. We addressed the completeness question with a multiple-step process. We (1) randomly selected 50 cases from the previously described population of 1,685 initially cleared industry personnel, (2) obtained paper files of the 50 investigative and adjudicative

[8] GAO-06-1070.

reports, (3) created a data collection instrument using federal investigative standards and adjudicative guidelines to standardize our data gathering, (4) sought experts' comments to refine our instrument and process, (5) coded data from the paper files, (6) had a second team member independently verify the information that another team member had coded, and (7) computed statistics to indicate the numbers of investigative and adjudicative reports with various types of missing documentation. In addition, two team members attended OPM's basic special agent training course to obtain an understanding of the investigative requirements as promulgated by OPM, and two other members of our team took about 40 hours of online adjudication training. We performed our original work from September 2005 through August 2006 in accordance with generally accepted government auditing standards.

Summary

At the time we issued our report in September 2006, our analysis of timeliness data showed that industry personnel contracted to work for the federal government waited more than 1 year on average to receive top secret security clearances and that timeliness statistics reported to Congress by OMB and OPM do not convey the full magnitude of the delays. Industry personnel granted eligibility for top secret clearance from DISCO from January to February 2006 waited an average of 446 days for their initial clearances and 545 days for their clearance updates. Delays were found in each phase of the clearance process that we examined. First, the application submission phase took an average of 111 days, nearly 100 days more than the government's goal. Inaccurate data that the employee provided in the application, multiple reviews of the application, and manual entry of some application forms are some of the causes for the extended application-submission phase. Second, the investigation phase took an average of 286 days for initial top secret clearances, well in excess of the 180-day goal. In addition, it took 419 days for top secret clearance updates (no goal is given for clearance update investigations). Factors contributing to the slowness of completing the investigation phase include an inexperienced investigative workforce and problems accessing national, state, and local records. Finally, it took DISCO adjudicators an average of 39 days to grant initial clearance eligibility to the industry personnel in our study population, compared to IRTPA's December 2006 requirement that 80 percent of all adjudication cases be completed in 30 days. Regardless of when in the process the delays occur, the outcome is the same—the government may incur additional costs from new industry employees being unable to begin work promptly and increased risks to national security because previously cleared industry employees are likely to continue working with critical information while it is determined whether they should still be eligible to hold a clearance. Moreover, the statistics that OMB and OPM report to Congress on the timeliness of the clearance process do not portray the full length of time it takes many applicants to receive clearances. We found several issues with the statistics, including limited information on reinvestigations for clearance updating and failure to measure the total time it took to complete the various phases of the clearance process. Statistics that underrepresent the time that it takes for investigations to be completed prevent Congress from having a full understanding of the government's efforts to decrease delays in the clearance process and determining if legislative actions are necessary.

In addition to delays in the clearance process, we found that that OPM provided incomplete investigative reports to DISCO adjudicators, which they used to determine top secret clearance eligibility. In our review of 50 initial investigations for top secret clearances randomly sampled from the population used in our timeliness analyses, we found that almost all (47 of 50) of the sampled investigative reports were missing documentation required by federal investigative standards. The missing data were of two general types: (1) the absence of documentation showing that an investigator had gathered all required information and (2) the absence of information to help resolve issues (such as conflicting information on indebtedness) that were raised in other parts of the investigative report. The federal standards indicate that investigations may be expanded as necessary to resolve issues. However, we found a total of 36 unresolved issues in 27 of the investigative reports. The most common unresolved issues pertained to financial consideration, foreign influence, and personal conduct. OPM officials suggested that the need to rapidly increase the size of the investigative workforce and prior quality control procedures that have since been replaced were some of the causes for the delivery of incomplete investigative reports to DISCO. Our review also found that DISCO adjudicators granted top secret eligibility to all 27 industry personnel whose investigative reports contained unresolved issues. In our November 2005 assessment of the government plan for improving the clearance process, we raised concerns about the limited attention devoted to assessing quality in the clearance process, but the plan has not been revised to address the shortcoming we identified.[9] The use of incomplete investigations and adjudications in the granting of top secret clearance eligibility increases the risk of unauthorized disclosure of classified

[9] GAO-06-233T.

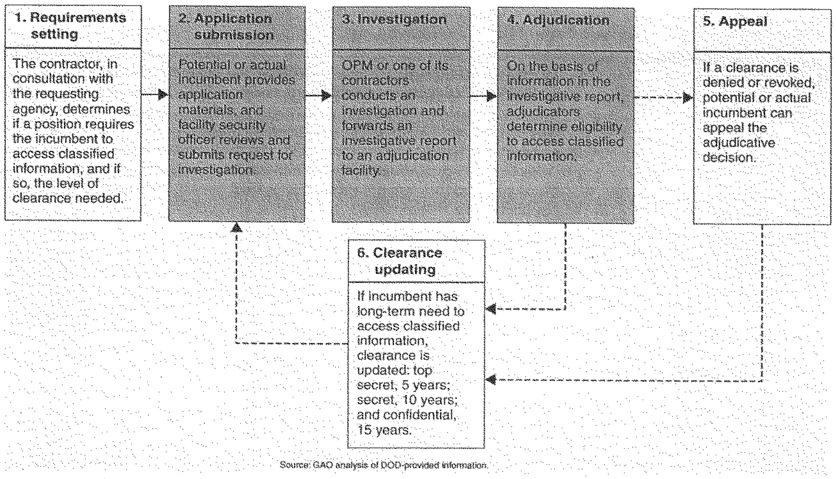
information. Also, it could negatively affect the government's efforts to move toward greater reciprocity. To improve the timeliness and completeness of investigations and adjudications, our report contained several recommendations to OMB.

Background

To ensure the trustworthiness, reliability, and character of personnel in positions with access to classified information, DOD relies on a multiphased personnel security clearance process.[10] Figure 1 shows six phases that could be involved in determining whether to grant an actual or a potential job incumbent a clearance. The three phases shown in gray are those that are most transparent to individuals requesting an initial clearance, and they are the three phases that were the primary focus of the findings in this testimony.

[10] DOD Directive 5200.2, *DOD Personnel Security Program* (Apr. 9, 1999), establishes policy and procedures for granting DOD military, civilian, and industry personnel access to classified information. Additionally, DOD Regulation 5200.2-R, *DOD Personnel Security Program* (January 1987), establishes DOD personnel security policies and procedures; sets forth standards, criteria, and guidelines upon which personnel security determinations shall be based; prescribes the types and scopes of personnel security investigations required; details the evaluation and adverse action procedures by which personnel security determinations shall be made; and assigns overall program management responsibilities. The policies and procedures for granting industry personnel security clearances and adjudicative procedural guidance for appealing cases if an unfavorable clearance decision is reached also are contained in DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Apr. 20, 1999).

Figure 1: Six Phases in the Personnel Security Clearance Process


1. Requirements setting
The contractor, in consultation with the requesting agency, determines if a position requires the incumbent to access classified information, and if so, the level of clearance needed.
2. Application submission
Potential or actual incumbent provides application materials, and facility security officer reviews and submits request for investigation.
3. Investigation
OPM or one of its contractors conducts an investigation and forwards an investigative report to an adjudication facility.
4. Adjudication
On the basis of information in the investigative report, adjudicators determine eligibility to access classified information.
5. Appeal
If a clearance is denied or revoked, potential or actual incumbent can appeal the adjudicative decision.
6. Clearance updating
If incumbent has long-term need to access classified information, clearance is updated: top secret, 5 years; secret, 10 years; and confidential, 15 years.

Source: GAO analysis of DOD-provided information.

Determining Top Secret Clearances for Industry Personnel Averaged More Than a Year, and Government Statistics Did Not Portray All Delays

At the time of our September 2006 report, our independent analysis of timeliness data showed that industry personnel contracted to work for the federal government waited more than 1 year on average to receive top secret security clearances, and government statistics did not portray the full length of time it takes many applicants to obtain clearances. We found delays in all phases of the clearance process that we examined, and government statistics did not account for the full extent of the delays. Delays in the clearance process may cost money and pose threats to national security (see table 1).

Table 1: Time Required to Grant Eligibility for a Top Secret Clearance to Industry Personnel—Cases Adjudicated in January and February 2006

		Phases of security clearance process [a]			
Total clearance process		2. Application submission	3. Investigation	4. Adjudication	
Clearance type	Average days[b]	Average days	Average days		Average days
Initial	446	111	286		39
Update	545	81	419		36
All	471	103	320		38
Example tasks and decisions required in each phase.		• Subject signs and dates the application. • Facility security officer checks application materials for completeness and accuracy, and forwards them to DISCO after any applicable changes. • DISCO adjudicator reviews materials for completeness and other concerns, and returns deficient materials to the facility security officer for further work. • If the application materials are approved, DISCO adjudicators determine whether the applicant is eligible for an interim clearance. • DISCO then forwards the completed application to OPM to begin the investigation. • OPM reviews the application for completeness and other concerns and returns deficient materials to DISCO for further work.	• If application is not submitted via eQIP, OPM key enters information for the application into its investigative database. • OPM schedules the investigation, assigning the investigation to its federal investigative workforce or one of its investigations contractors. • Investigators gather information on the individual in order to produce an investigative report. • OPM's PIPS database obtains a variety of electronic information that is available via government databases. • Once the investigative work has been completed, OPM checks the investigative report for completeness before sending the report to an adjudication facility.	• OPM prints a paper copy of the investigative report. • OPM ships the paper copy of the report to the adjudication facility if the agency chose that format or cannot get it electronically.[c]	• DISCO adjudicator reviews the information in the investigative report. • DISCO adjudicator determines if industry employee is eligible for a clearance. [d]

Source: GAO analysis of OPM and DOD information.

Legend: PIPS = OPM's Personnel Investigations Processing System.

[a] The phases referred to here are based on those in figure 1.

[b] The average days for the phases do not sum to the average days for the total clearance process because the number of applicable cases varies for each calculation.

[c] According to OPM, the requesting agency has the option to request that the investigation be delivered through PIPS, eliminating the mail time, for all completed investigations that do not contain hard-copy third-party information.

[d] Additional time may be needed in this phase if DISCO adjudicators identify major security issues in the investigative report. Such cases may be submitted to DOHA for the clearance eligibility determination.

Delays in Determining Eligibility Are Caused by Many Factors

As table 1 shows, industry personnel granted eligibility for top secret clearances from DISCO from January to February 2006 waited an average of 446 days for their initial clearances or 545 days for their clearance updates. DOD may, however, have issued interim clearances to some of these industry personnel, which might have allowed them to begin work before they received their final clearances. IRTPA requires that beginning in December 2006, 80 percent of clearances be completed in an average of 120 days. Delays were found in each phase of the clearance process that we examined:

- *Application submission.* The application-submission phase of the clearance process took an average of 111 days for the initial clearances that DISCO adjudicated in January and February 2006 (see table 1). The starting point for our measurement of this phase was the date when the application was submitted by the facility security officer. Our end point for this phase was the date that OPM scheduled the investigation into its Personnel Investigations Processing System. We used this starting date because the government can begin to incur an economic cost if an industry employee cannot begin work on a classified contract because of delays in obtaining a security clearance and this end date because OPM currently uses this date as its start point for the next phase in the clearance process. The government plan for improving the clearance process noted that "investigation submission" (i.e., application submission) is to be completed within an average of 14 calendar days or less. Therefore, the 111 days taken for the application-submission phase was nearly 100 more days on average than allocated. Several factors contributed to the amount of time we observed in the application-submission phase, including rejecting applications multiple times because of inaccurate information (as reported in an April 2006 DOD Office of Inspector General report); multiple completeness reviews—the corporate facility security officer, DISCO adjudicators, and OPM staff; and manually entering data from paper applications if eQIP was not used.

- *Investigation.* Investigations for the initial top secret clearances of industry personnel adjudicated in January and February 2006 took an average of 286 days, compared to OMB's 180-day goal for that period (see table 1). During the same period, investigations for top secret clearance updates or "reinvestigations" took an average of 419 days, almost one and a half times as long as the initial investigations (no goal is given for clearance updates or reinvestigations). The mandated February 2007 OMB report to Congress noted that "Reinvestigation timeliness has not been addressed, because the improvement effort focused on individuals for whom initial security clearances are required to perform work." Our September 2006 report identified many factors that inhibited the speed with which OPM can deliver investigative reports to DISCO and other adjudication facilities. Those causes included backlogged cases that prevent the prompt start of work on new cases, the relative inexperience of the investigative workforce, slowness in developing the capability to investigate overseas leads, and difficulty obtaining access to data in governmental records.

- *Adjudication.* DISCO adjudicators took an average of 39 days to grant initial clearance eligibility to the industry personnel in our population (see table 1). The measurement of this phase for our analysis used the same start and stop dates that OPM uses in its reports, starting on the date that OPM closed the report and continuing through the date that DISCO adjudicators decided clearance eligibility. IRTPA requires that at least 80 percent of the adjudications made from December 2006 through December 2009 be completed within an average of 30 days. As of June 2006, DISCO reported that it had adjudicated 82 percent of its initial top secret clearances within 30 days.

Delays in any phase of the clearance process cost money and threaten national security. Delays in completing initial security clearances may have a negative economic impact on the costs of performing classified work within or for the U.S. government. For example, in a May 2006 congressional hearing, a representative of a technology association testified that retaining qualified personnel resulted in salary premiums as high as 25 percent for current clearance holders.[11] Delays in completing clearance updates can have serious but different negative consequences than those stemming from delays in completing initial clearance-eligibility determinations. In 1999, the Joint Security Commission reported that delays in initiating reinvestigations for clearance updates create risks to national security because the longer individuals hold clearances the more likely they are to be working with critical information.

[11] Doug Wagoner, statement for the record, hearing before the Committee on Government Reform, U.S. House of Representatives (May 17, 2006).

OMB's and OPM's Timeliness Reporting Does Not Convey Full Magnitude of Delays

The statistics that OMB and OPM have provided to Congress on the timeliness of the personnel security clearance process do not convey the full magnitude of the investigation-related delays facing the government. While our September 2006 report noted additional problems with the transparency of the timeliness statistics, I will review our concerns about five such issues: (1) limited information on reinvestigations for clearance updating, (2) not counting the total number of days to finish the application-submission phase, (3) shifting some investigation-related days to the adjudication phase or not counting them, (4) not counting the total number of days to complete closed pending cases, and (5) not counting the total number of days to complete investigations sent back for rework.

Limited information on reinvestigations for clearance updating. In its mandated February 2007 report to Congress, OMB acknowledged that "reinvestigation timeliness has not been addressed," but the findings from our population of industry personnel (obtained using DOD's, instead of OPM's, database to assess timeliness) indicated that clearance update reinvestigations took about one and a half times as long as the initial investigations. The absence of timeliness information on clearance update reinvestigations does not provide all stakeholders—Congress, agencies, contractors attempting to fulfill their contracts, and employees awaiting their clearances—with a complete picture of clearance delays. We have noted in the past that focusing on completing initial clearance investigations could negatively affect the completion of clearance update reinvestigations and thereby increase the risk of unauthorized disclosure of classified information.

Not counting all days to finish the application-submission phase. OMB's February 2007 report noted that its statistics do not include "the time to hand-off applications to the investigative agency." The gray section of the application-submission phase in table 1 shows some of the activities that were not counted when we examined January and February 2006 clearance documentation for industry personnel. These activities could be included in timeliness measurements depending on the interpretation of what constitutes "receipt of the application for a security clearance by an authorized investigative agency"—IRTPA's start date for the investigation phase.

Shifting some investigation-related days to the adjudication phase or not counting them. In our September 2006 report, we raised concerns about how the time to complete the adjudication phase was measured. The activities in the gray section of the adjudication phase in table 1 show that the government's procedures for measuring the time required for the adjudication phase include tasks that occur before adjudicators actually receive the investigative reports from OPM. More recently, OMB's February 2007 report to Congress noted that its timeliness statistics do not include "the time to ... hand-off investigation files to the adjudicative agency" and estimated this handling and mailing time at up to 15 days.

Not counting all days for closed pending cases. OPM's May 2006 testimony before Congress did not indicate whether the timeliness statistics on complete investigations included a type of incomplete investigation that OPM sometimes treats as being complete. In our February 2004 report, we noted that OPM's issuance of "closed pending" investigations—investigative reports sent to adjudication facilities without one or more types of source data required by the federal investigative standards—causes ambiguity in defining and accurately estimating the backlog of overdue investigations. In our February 2004 report, we also noted that cases that are closed pending the provision of additional information should continue to be tracked separately in the investigation phase of the clearance process. According to OPM, from February 20, 2005, through July 1, 2006, the number of initial top secret clearance investigative reports that were closed pending the provision of additional information increased from 14,841 to 18,849, a 27 percent increase. DISCO officials and representatives from some other DOD adjudication facilities have indicated that they will not adjudicate closed pending cases since critical information is missing. OPM, however, has stated that other federal agencies review the investigative reports from closed pending cases and may determine that they have enough information for adjudication. Combining partially completed investigations with fully completed investigations overstates how quickly OPM is supplying adjudication facilities with the information they require to make their clearance-eligibility determinations.

Not counting all days when inadequate investigations are returned. OMB's February 2007 report stated that its statistics do not include the time incurred to "return the files to the investigative agency for further information." OPM's procedure is to restart the measurement of investigation time for the 1 to 2 percent of investigative reports that are sent back for quality control reasons, which does not hold OPM fully accountable for total investigative time when deficient products are delivered to its customers. In fact, restarting the time measurement for reworked investigations could positively affect OPM's statistics if the reworked sections of the investigation take less time than did the earlier effort to complete the large portion of the investigative report.

IRTPA establishes timeliness requirements for the security clearance process. Specifically, it states that "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." IRTPA did not identify situations that could be excluded from mandated timeliness assessments. Without fully accounting for the total time needed to complete the clearance process, Congress will not be able to accurately determine whether agencies have met IRTPA-mandated requirements or determine if legislative actions are necessary.

OPM Delivered Incomplete Investigative Reports, and DISCO-Adjudicated Cases Did Not Document All Clearance-Determination Considerations

OPM provided incomplete investigative reports to DOD adjudicators, which they used to determine top secret clearance eligibility. Almost all (47 of 50) of the sampled investigative reports we reviewed were incomplete based on requirements in the federal investigative standards. In addition, DISCO adjudicators granted clearance eligibility without requesting additional information for any of the incomplete investigative reports and did not document that they considered some adjudicative guidelines when adverse information was present in some reports. Granting clearances based on incomplete investigative reports increases risks to national security. In addition, use of incomplete investigative reports and not fully documenting adjudicative considerations may undermine the government's efforts to increase the acceptance of security clearances granted by other federal agencies.

Almost All of the Sampled Investigative Reports Were Incomplete

In our review of 50 initial investigations randomly sampled from the population used in our timeliness analyses, we found that 47 of 50 of the investigative reports were missing documentation required by the federal investigative standards. The missing data were of two general types: (1) the absence of documentation showing that an investigator gathered the prescribed information in each of the applicable 13 investigative areas and included requisite forms in the investigative report and (2) the absence of information to help resolve issues (such as conflicting information on indebtedness) that were raised in other parts of the investigative report. The requirements for gathering these types of information were identified in federal investigative standards published about a decade ago.

At least half of the 50 reports did not contain the required documentation in 3 investigative areas: residence (33 of 50), employment (32), and education (27). In addition, many investigative reports contained multiple deficiencies within each of these areas. For example, multiple deficiencies might be present in the residence area because investigators did not document a rental record check and an interview with a neighborhood reference. Moreover, 44 of the 50 investigative reports had 2 to 6 investigative areas out of a total of 13 areas with at least one piece of missing documentation.

We also found a total of 36 unresolved issues in 27 of the investigative reports. The three investigative areas with the most unresolved issues were financial consideration (11 of 50 cases), foreign influence (11), and personal conduct (7). Federal standards indicate that investigations may be expanded as necessary to resolve issues. According to OPM, (1) issue resolution is a standard part of all initial investigations and periodic reinvestigations for top secret clearances and (2) all issues developed during the course of an investigation should be fully resolved in the final investigative report provided to DOD.

One investigative report we examined serves as an example of the types of documentation issues we found during our review. During the course of this particular investigation, the subject reported having extramarital affairs; however, there was no documentation to show that these affairs had been investigated further. Also, the subject's clearance application indicated cohabitation with an individual with whom the subject had previously had a romantic relationship, but there was no documentation that record checks were performed on the cohabitant. Moreover, information in the investigative report indicated that the subject had defaulted on a loan with a balance of several thousand dollars; however, no other documentation suggested that this issue was explored further. When we reviewed this and other deficient investigative reports with OPM Quality Management officials, they agreed that the investigators should have included documentation to resolve the issues.

While we found that the interview narratives in some of the 50 OPM investigative reports were limited in content, we did not identify them as being deficient for the purposes of our analysis because such an evaluation would have required a subjective assessment that we were not willing to make. For example, in our assessment of the presence or absence of documentation, we found a 35-word narrative for a subject interview of a naturalized citizen from an Asian country. It stated only that the subject did not have any foreign contacts in his birth country and that he spent his time with family and participated in sports. Nevertheless, others with more adjudicative expertise voiced concern about the issue of documentation adequacy. Top officials representing DOD's adjudication facilities with whom we consulted were in agreement that OPM-provided investigative summaries had been inadequate.

When we reviewed our findings in meetings with the Associate Director of OPM's investigations unit and her quality management officials they cited the inexperience of the rapidly expanded investigative workforce and variations in training provided to federal and contractor investigative staff as possible causes for the incomplete investigative reports we reviewed. Later, in official agency comments to our September 2006 report, OPM's Director indicated that some of the problems that we reported were the result of transferred staff and cases when OPM accepted DOD investigative functions and personnel. However, OPM had had 2 years to prepare for the transfer between the announced transfer agreement in February 2003 and its occurrence in February 2005. Furthermore, the staff and cases were under OPM control until the investigative reports were subsequently transferred to OPM for adjudication in January or February of 2006. In addition, 47 of the 50 investigative reports that we reviewed were missing documentation even though OPM had quality control procedures for reviewing the reports before they were sent to DOD.

In our November 2005 testimony evaluating the government plan for improving the personnel security clearance process, we stated that developers of the plan may wish to consider adding other indicators of the quality of investigations. During our review, we asked the Associate Director of OPM's Investigations Unit if OMB and OPM had made changes to the government plan to address quality measurement and other shortcomings we identified. OPM's Associate Director said that the plan had not been modified to address our concerns but that implementation of the plan was continuing.

DISCO Adjudicators Granted Top Secret Clearance Eligibility for Cases with Missing Information

Our review found that DISCO adjudicators granted top secret clearance eligibility for all 47 of the 50 industry personnel whose investigative reports did not have full documentation. In making clearance-eligibility determinations, the federal guidelines require adjudicators to consider (1) guidelines covering 13 specific areas, such as foreign influence and financial considerations; (2) adverse conditions or conduct that could raise security concerns and factors that might mitigate (alleviate) the condition for each guideline; and (3) general factors related to the whole person. According to a DISCO official, DISCO and other DOD adjudicators are to record information relevant to each of their eligibility determinations in JPAS. They do this by selecting applicable guidelines and mitigating factors from prelisted responses and may type up to 3,000 characters of additional information.

The adjudicators granted eligibility for the 27 industry personnel whose investigative reports (discussed in the prior section) contained unresolved issues without requesting additional information or documenting in the adjudicative report that the information was missing. The following is an example of an unresolved foreign influence issue, which was not documented in the adjudicative report, although DISCO officials agreed that additional information should have been obtained to resolve the issue before the individual was granted a top secret clearance. A state-level record check on an industry employee indicated that the subject was part owner of a foreign-owned corporation. Although the DISCO adjudicator applied the foreign influence guideline for the subject's foreign travel and mitigated that foreign influence issue, there was no documentation in the adjudicative report to acknowledge or mitigate the foreign-owned business. When we asked why adjudicators did not provide the required documentation in JPAS, the DISCO officials as well as adjudication trainers said that adjudicators review the investigative reports for sufficient documentation to resolve issues and make judgment calls about the amount of risk associated with each case by weighing a variety of past and present, favorable and unfavorable information about the person to reach an eligibility determination.

Seventeen of the 50 adjudicative reports were missing documentation on a total of 22 guidelines for which issues were present in the investigative reports. The missing guideline documentation was for foreign influence (11), financial considerations (5), alcohol consumption (2), personal conduct issues (2), drug involvement (1), and foreign influence (1). DISCO officials stated that procedural changes associated with JPAS implementation contributed to the missing documentation. DISCO began using JPAS in February 2003, and it became the official system for all of DOD in February 2005. Before February 2005, DISCO adjudicators were not required to document the consideration of a guideline issue unless the adverse information could disqualify an individual from being granted a clearance eligibility. After JPAS implementation, DISCO adjudicators were trained to document in JPAS their rationale for the clearance determination and any adverse information from the investigative report, regardless of whether an adjudicative guideline issue could disqualify an individual from obtaining a clearance. The administrators also attributed the missing guideline documentation to a few adjudicators attempting to produce more adjudication determinations.

Delivery and Use of Incomplete Investigations Increase Risks to National Security and Reciprocity

Decisions to grant clearances based on incomplete investigations increase risks to national security because individuals can gain access to classified information without being vetted against the full federal standards and guidelines. Furthermore, if adjudication facilities send the incomplete investigations back to OPM for more work, the adjudication facilities must use adjudicator time to review cases more than once and then use additional time to document problems with the incomplete investigative reports.

Incomplete investigations and adjudications undermine the government's efforts to move toward greater clearance and access reciprocity. An interagency working group, the Security Clearance Oversight Steering Committee, noted that agencies are reluctant to be accountable for poor quality investigations, adjudications conducted by other agencies or organizations, or both. To achieve fuller reciprocity, clearance-granting agencies need to have confidence in the quality of the clearance process. Without full documentation of investigative actions, information obtained, and adjudicative decisions, agencies could continue to require duplicative investigations and adjudications.

Concluding Observations

Incomplete timeliness data limit the visibility of stakeholders and decision makers in their efforts to address long-standing delays in the personnel security clearance process. For example, not accounting for all of the time used when personnel submit an application multiple times before it is accepted limits the government's ability to (1) accurately monitor the time required for each step in the application-submission phase and (2) identify positive steps that facility security officers, DISCO adjudicators, OPM investigative staff, and other stakeholders can take to speed the process. The timeliness-related concerns identified in my testimony show the fragmented approach that the government has taken to addressing clearance problems. When I testified before this Subcommittee in November 2005, we were optimistic that the government plan for improving the clearance process prepared under the direction of OMB's Deputy Director for Management would be a living document that would provide the strategic vision for correcting long-standing problems in the personnel security clearance process. However, nearly 2 years after first commenting on the plan, we have not been provided with a revised plan that lays out how the government intends to address the shortcomings that we identified in the plan during our November 2005 testimony. Continued failure to address the shortcomings we have cited could significantly limit the positive impact that the government has made in other portions of the clearance process through improvements such as hiring more investigators and promoting reciprocity.

While eliminating delays in the clearance process is an important goal, the government cannot afford to achieve that goal by providing investigative and adjudicative reports that are incomplete in the key areas required by federal investigative standards and adjudicative guidelines. Also, the incomplete investigative and adjudicative reports could suggest to some security managers that there is at least some evidence to support agencies' concerns about the risks that may come from accepting the clearances issued by other federal agencies, and thereby negatively affect OMB's efforts toward achieving greater reciprocity. Further, as we pointed out in November 2005, the almost total absence of quality metrics in the governmentwide plan for improving the clearance process hinders Congress's oversight of these important issues. Finally, the missing documentation could have longer-term negative effects, such as requiring future investigators and adjudicators to devote time to obtaining the documentation missing from current reviews when it is time to update the clearances currently being issued.

Mr. Chairman and Members of the Subcommittee, this concludes my prepared statement. I would be happy to answer any questions you may have at this time.

Contact and Acknowledgments

For further information regarding this testimony please contact me at (202)512-5559 or stewartd@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals who made key contributions to this testimony are Jack E. Edwards, Assistant Director; Kurt A. Burgeson; Nicolaas C. Cornelisse; Alissa H. Czyz; Ronald La Due Lake; Beverly C. Schladt; and Karen D. Thornton.

Related GAO Products

DOD Personnel Clearances: Questions and Answers for the Record Following the Second in a Series of Hearings on Fixing the Security Clearance Process. GAO-06-693R. Washington, D.C.: June 14, 2006.

DOD Personnel Clearances: New Concerns Slow Processing of Clearances for Industry Personnel. GAO-06-748T. Washington, D.C.: May 17, 2006.

DOD Personnel Clearances: Funding Challenges and Other Impediments Slow Clearances for Industry Personnel. GAO-06-747T. Washington, D.C.: May 17, 2006.

GAO's High-Risk Program. GAO-06-497T. Washington, D.C.: March 15, 2006.

Questions for the Record Related to DOD's Personnel Security Clearance Program and the Government Plan for Improving the Clearance Process. GAO-06-323R. Washington, D.C.: January 17, 2006.

DOD Personnel Clearances: Government Plan Addresses Some Long-standing Problems with DOD's Program, But Concerns Remain. GAO-06-233T. Washington, D.C.: November 9, 2005.

Defense Management: Better Review Needed of Program Protection Issues Associated with Manufacturing Presidential Helicopters. GAO-06-71SU. Washington, D.C.: November 4, 2005.

Questions for the Record Related to DOD's Personnel Security Clearance Program. GAO-05-988R. Washington, D.C.: August 19, 2005.

DOD Personnel Clearances: Some Progress Has Been Made but Hurdles Remain to Overcome the Challenges That Led to GAO's High-Risk Designation. GAO-05-842T. Washington, D.C.: June 28, 2005.

DOD's High-Risk Areas: Successful Business Transformation Requires Sound Strategic Planning and Sustained Leadership. GAO-05-520T. Washington, D.C.: April 13, 2005.

High-Risk Series: An Update. GAO-05-207. Washington, D.C.: January 2005.

STATEMENT
OF
MR. TIMOTHY R. SAMPLE
PRESIDENT
INTELLIGENCE AND NATIONAL SECURITY ALLIANCE
TO
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS COMMITTEE
SUBCOMMITTEE ON OVERSIGHT OF GOVERNMENT MANAGEMENT, THE FEDERAL WORKFORCE AND THE DISTRICT OF COLUMBIA

Evaluating Progress and Identifying Obstacles in Improving the Federal Government's Security Clearance Process

May 17, 2007

Chairman Akaka, Mr. Voinovich, and Members of the Committee, I am honored to be in front of you this morning to discuss this vitally important issue. I commend the subcommittee for taking on this task, as I believe the personnel security clearance process is at the core of several issues that go well beyond whether an individual should have access to classified information. In fact, the personnel security process and the security culture upon which it is based is responsible for fueling government acquisition processes that unnecessarily cost the government and the American taxpayers billions and for our inability to get the most desired and needed individuals into key positions in government. It was also an important factor in the government's inability to share intelligence between agencies and departments prior to the terrorists' attacks on September 11, 2001.

Mr. Chairman, I am the President of the Intelligence and National Security Alliance (INSA), which is a non-profit, non-partisan, professional association that focuses on a variety of issues related to national security, especially issues confronting our intelligence capabilities. Although the bulk of our membership is based on corporate contributions, INSA is not a trade association – we do not lobby on behalf of a certain set of companies or for specific programs. Instead, INSA operates as a public policy forum aimed at educating government and the public about key issues confronting our national security structures and capabilities. We utilize our individual and corporate membership to access a wealth of expertise and expand our networks in order to provide the best insight and advice to government agencies and to the American people. In general, INSA advocates for strong, robust intelligence capabilities in order to ensure our nation's security. It is with this in mind that INSA, and its Council on Security and Counterintelligence, has studied the issues that the Committee is confronting today. Our experience stems from the network of expertise found in our Council as well as from a history of study from our predecessor organization, the Security Affairs Support Association (SASA). The INSA Council on Security is in the process of completing a white paper on the need to transform the personnel security clearance process. Several of my remarks come from our assessments. I will send copies of this white paper to the Committee once completed, and I hope that you will consider its points in your overall deliberations. With this background in mind, let me turn to the issues at hand.

Mr. Chairman, you have chosen to title this hearing: *Evaluating Progress and Identifying Obstacles in Improving the Federal Government's Security Clearance Process.* I will structure my remarks to respond to these two issues you raised: how have we progressed in our security clearance procedures, and what are the obstacles to improving our security processes? As I will detail throughout my remarks below, despite recent attempts at reform, there has been no appreciable difference in the security clearance situation. One need only look at the average clearance processing times, even the cheery and creatively calculated averages, to see that the backlog and processing times have not improved, and perhaps worsened, during this decade.

In response to the question of obstacles to improvement, we agree with the Security Clearance Reform Coalition's (of which we are a member) conclusions that technology needs to be employed in the process, agencies must stop crafting their own requirements for mutual recognition of clearances, among others. We can add more obstacles to this list, including an outdated field investigation; agencies that refuse to honor other agencies' equivalent clearances; and clearances that are tied to agencies as opposed to the individual.

At a minimum, Congress should strongly consider implementation of the Coalition's recommendations. But in doing so, you must understand that you end up with a more efficient flawed system. Although these improvements are important, they are not sufficient to fix the root cause of this broken system: a culture steeped in risk avoidance. As I will explain further, this culture of risk avoidance causes an immense backlog of initial clearances, neglects the re-investigation process of cleared personnel, and incentivizes security officers against clearing first and second generation Americans and those with extensive foreign travel and contacts, despite overwhelming evidence that those individuals have the expertise our intelligence community and government desperately need.

Evaluating Progress in the Security Clearance Process

Invariably, recent discussions about security clearances focus on the issues of the backlog of individuals awaiting clearances, which number in the hundreds of thousands, and the time it takes to "clear" them. Congress itself, in the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), focused on such numerical measures of merit when it directed that government agencies achieve average timelines of 90 days for investigations and 30 days for adjudication for 80 percent of all initial clearances.

Although I would strongly urge the Committee to go well beyond these two data points – as I will later in this testimony – I would like to start with these areas of debate.

First, a testament to the inefficiencies of the current process is that valid metrics cannot be derived due to the lack of transparency within the system, the lack of compatible systems between and among agencies and departments, the fragmented nature of the process, and the intensity of manual labor demanded by the current processes. As a result, so-called authoritative numbers that are delivered by the Office of Personnel Management (OPM), the Government Accounting Office (GAO), the Department of Defense (DoD), or other entities must be considered to be like political polling numbers – highly subject to interpretation depending on what outcome is desired. The September 2006 GAO report on DoD Personnel Clearances provides a prime example: the appendices contain letters written by OPM and OMB disputing the methods and calculations in the report.

This is not meant as a criticism of those presenting the data, as much as recognition that the current process does not allow for valid, unbiased empirical data to be collected. OPM's Security Clearance Oversight Group report in February of this year projected timelines suggesting that IRTPA investigation and adjudication goals will be met this year by OPM, while the recent GAO report stated the OPM averages 446 days was required for initial clearances, far above IRPTA's mandated 120 day average. In considering the OPM report's data, we note what is not considered in the evaluations. Specifically, the report notes that the timelines do not consider the application process – that is the time from when an individual fills out the necessary forms until the "case file" is declared ready for investigation by the investigative agency. This is a critical aspect of the investigation in that many cases have significant delays if the application data is incomplete or if all the data doesn't arrive into the case file due to the extent of reliance on a very manual process. Moreover, your constituents awaiting clearances don't care which part of the process is considered in these goals and evaluations. They just know that they continue to wait an unreasonable amount of time to get a clearance and go to work.

The report also notes that the reinvestigations are not addressed. This is because the main focus of agencies, and of Congress, since September 11, 2001 has been on obtaining initial clearances for the large numbers of new government employees and contractors required. This is specifically important because, by focusing government efforts on initial investigations, significant security risks are being created by a growing backlog in periodic reinvestigations. In fact, the recent GAO report indicates that the average timelines for reinvestigations are now up to 545 days. Consequently, although the government has attempted to improve some aspects of the existing process, the results are marginal and misleading.

Identifying Obstacles in the Security Clearance Process

Today, the personnel clearance process that we utilize in government and industry is not that different from when it was implemented some 60 years ago. The security clearance process relies on a front-end investigation and, once cleared, the individual is not regularly re-investigated for at least five years. All agencies follow investigative and adjudicative standards established by a series of laws and executive orders, but many have additional agency-specific policies and processes, increasing the difficulty in reciprocity. Furthermore, the field investigation process is less effective than it once was. Although some pieces of valuable information can be discovered in some cases during an investigation, our society has changed to the point that in most cases more information about you can be derived from available databases than from asking your neighbor whether or not you live within your means.

Overall, this current process can be referred to as "risk avoidance," whereby thorough investigations of individuals are conducted prior to allowing them access to classified information. We refer to it as risk avoidance because the emphasis is placed on the initial vetting. Does the candidate have bad credit or a drinking problem? Does the candidate have extensive foreign contacts or a mental disorder? While none of these factors individually or together guarantees that an individual will misuse, sell, or give away our nation's secrets, the risk avoidance process argues that if an individual initially passes these criteria, they are less likely to do so. The "risk avoidance" process flourished and arguably adequately protected our nation's secrets, albeit with some notable, damaging exceptions.

The risk avoidance culture and system has some damaging repercussions for security and counterintelligence today. First and foremost, the emphasis is placed on the initial investigation, but not nearly enough on the monitoring or reinvestigation of those who already have access to classified information. This is a dangerous oversight. The most high-profile spy cases of the past 15 years have been committed by those who have had access to classified information for decades, not those who just got in the door. Ana Montes worked for the DIA for 16 years when she was caught spying for Cuba; Robert Hanssen had 25 years at the FBI. Aldrich Ames worked for the CIA for 23 years before he walked into the Soviet Embassy in Washington and offered to spy against the United States, which he did for nine years before his capture in 1994. All three spied under the same system we are evaluating today.

Individuals with security clearances are nominally reinvestigated every five years, a term that is becoming longer because of the backlog. Because of this focus on initial clearances, we are creating inherent security risks by taking away critical resources that currently make up our principal capability of revealing breaches in security at an individual level. Because of this, it is, unfortunately, not unreasonable to contemplate that another Ames, Montes or Hanson might be able to continue spying while their reinvestigation is caught up in the clearance backlog.

A second outcome of the risk avoidance culture is our inability to get the right people in the right job when we need them. As I mentioned before, our risk avoidance security culture discourages hiring first and second generation Americans for classified positions because they have foreign contacts, such as family living in a foreign country. While everyone seems to agree that these individuals have the language skills and cultural understanding that are vitally important in today's world, our risk avoidance security culture dictates that these individuals are too risky to be granted access to classified information. It is a sad reality that, even in this era of global business and world-wide terrorism, our security process is highly slanted to hire individuals who have read a book about a country than someone who has actually been there. Put another way, with the philosophy of today's security clearance process, we likely would not hire those individuals who were so critical in breaking Japanese codes in World War II or building the atomic bomb.

The impact on industry supporting government is also substantial. Private sector contractors have a difficult time filling positions that the government requests. The government's security and acquisition processes have created a market in which a contractor is almost forced to hire personnel based on whether he or she has clearance, rather than supplying the best possible candidate. Ultimately, industry then charges the costs engendered because of these issues back to the government, driving up government contract costs well beyond what should be necessary.

In order to meet the requirements of today's acquisition process, industry must hire individuals for specific contracts and then submit them for clearances should they win the contract. This means that industry must not only have someone on their books for over a year, but they must find these individuals something to do while they wait. In some cases, there may be other, unclassified, contracts on which they can work. If not, these individuals get assigned "busy work" and are paid out of companies' overhead funds. In other cases, the individual may leave the company before contract award because they have found more meaningful work with some other company that can put them to work right away. In still other cases, industry will only bid "cleared" individuals in their employment with the hope of being able to replace them with new individuals as those individuals' clearances are finally granted.

The second aspect of the impact of the current process is that a premium has now been placed on hiring individuals with security clearances. In some cases, significant bonuses and a salary structure that can be up to 35% higher than someone without a clearance have been experienced. Consequently, the competition to entice an individual from one company to another, or from government to a company, is intense. The results can be an unstable government workforce as well as an unstable acquisition process as programs experience a revolving door of individuals throughout the period of performance.

The Solution: A New Security Paradigm

Mr. Chairmen, I have outlined for you a few of the reasons why our 60-year-old personnel clearance system is not only inefficient but ineffective in providing the United States with the security it needs. Our risk avoidance culture is based on threats, societies, and a pace that is well in our past. Not only do we not take advantage of technology, we are hindered by it. We attempt to avoid risk in a desire to achieve unachievable goals of absolute security, and in the process we are now creating vulnerabilities for others to capitalize on. Today, companies around the world have understand that risk cannot be avoided, but must be managed. It is past time for our government to adopt the same philosophy.

We propose moving from a "risk avoidance" security culture to one based on "risk management." In a risk management culture, the system acknowledges the element of risk at the beginning of the process, but instead has mechanisms that would allow that risk to be mitigated because of a robust ability to detect issues on a day-to-day basis. Examples of such a culture can be found in the financial marketplace where companies generally "clear" their employees – who arguably handle extremely sensitive financial information that can equate in sensitivity to much of our "classified" national security secrets – within two weeks. Afterward, however, there is a process of continuous evaluation and compliance that ensures adherence to the stringent guidelines warranted by the sensitivity of the data. The financial sector's ability to "clear" individuals so quickly is based on a fully automated system of extensive record and data base checks that, in today's world can present a detailed understanding of someone's life; such a detailed picture would be as revealing as information derived from a field investigation, if not more so, and in a small fraction of the time. This initial clearance is followed up by a continuous monitoring and evaluation process that mitigates further risk.

An example of the "continuous evaluation" process (as well as reciprocity) can again be found in the financial sector, this time in the credit card area. If I were in Sydney, Australia today, I could take my Visa Card and put it into an ATM machine. The machine would read the date on the card, compare it with a data base of financial records and, having established the legitimacy of the card would respond and "say" "G'day, Tim." I could then take out significant amounts of money and walk away. In this scenario, the banking industry has taken on an element of risk. First, that I have money in the account or an available credit balance, which is quickly ascertained by data base checks before the money is given. A second element of risk is whether or not the legitimate card holder is presenting this card. To mitigate that risk, there is a continuous evaluation aspect that runs silently in the background and monitors my account/card usage. Should something out of the ordinary – as defined by my normal spending habits that have been monitored – transpires, action is taken, usually by a telephone call to me asking about recent purchases in order to either confirm that everything is alright or to identify a breech in security of the system. In most cases, such credit card or identity theft is quickly identified and acted upon. An example of reciprocity in the system is that I can walk up to any ATM machine in Sydney, or anywhere else in the world, regardless of whether it is "my" bank and have the same result.

Mr. Chairman, there is no reason that the government could not adopt similar processes for granting security clearances as those I've just described and virtually wipe out backlogs as well as increase our overall security. Such a system could allow the government to immediately determine suitability and grant or decline a clearance to the majority of applicants, and employ traditional field investigations when necessary. Although the level of clearance required for an individual's initial application would be based on a specific job, once obtained the clearance would be assigned to the individual for his lifetime and would be continuously monitored and adjusted based on a continuing assessment and evaluation process. The elements of such a system would include:

- A fully automated, government-wide application systems, including electronic fingerprinting.
- A centralized, automated investigation that would perform significantly robust database checks on applicants in order to create a "score" assessing a level of risk, much like your credit score. Such database checks would far exceed today's National Agency Check with Law and Credit (NACLC), currently required for SECRET and TOP SECRET clearances, and be more robust than current data collected from most field investigations.
- An automated adjudication system that would take an applicant's score and compare it with the acceptable level of vulnerability for the specific job for which the individual applied. Should the scores compare favorably, a clearance would be granted. For those that do not compare favorably, the system would generate a human adjudication process, which could also lead to a field investigation.
- An automated, continuous evaluation system that would run in the background and would adjust an individual's score on a near-real time basis. Such an evaluation would detect significant changes or deviations that would trigger an investigation, depending upon the risk and vulnerability assessments of the job.
- A system of aperiodic investigations. Such investigations may be completely random, based on the vulnerability or sensitivity of a specific position, or may be triggered by detection of an anomaly through the continuous evaluation process.
- A robust, government-wide counterintelligence process that would compliment this new system by assessing the threat environment and monitoring developments that would be linked to certain jobs, facilities, and programs.
- All systems would be based primarily on newly purchased commercial-off-the-shelf (COTS) technology, phasing out existing legacy systems as rapidly as possible
- The overall process would be governed by a new set of government-wide laws, regulations, Executive Orders, and standards.

Such a system would reallocate human resources. Although there would be some human investigations and adjudication associated with the initial investigations, the bulk of these resources would be shifted to incident and aperiodic reinvestigations, thus increasing security in areas where we are most vulnerable today.

Mr. Chairman, let me stress that this is not a cost savings plan, at least in the near term. Security cannot be accomplished "on the cheap." Resource "savings" from limiting the number of initial field investigations, would be allocated to those areas where we can best mitigate risk through aperiodic reinvestigations. That said I believe that over time the government would save considerable expense in terms of opportunity costs associated with working for the government. Nor would implementation be simple. I do believe, however, that it is obtainable. Finally, I must emphasize the need to incentivize security officers to adopt such a dramatic cultural change.

Creating such a system will require resolve, especially at the senior levels of the Executive and Legislative Branches. Heretofore, government leaders have relegated security to an administrative function. Only recently have they begun to fully understand the significant impact of the processes itself as well as the bureaucracy that supports it. For the first time, senior leaders in the Department of Defense, the Intelligence Community, the White House, and other departments of government have are coming to an understanding that there must be significant and dramatic changes to the personnel security clearance process. These efforts will be enhanced by Congress' continued focus. I appreciate this development and believe that now is the time for dramatic transformation.

Conclusion and the Need to Act Now

Mr. Chairman, it has been just over one year since the Defense Security Service (DSS) announced that they were suspending the acceptance and processing of industry clearances because they were out of funding. Since that time, I can find no improvements to the overall government clearance process that would prevent a recurrence of such a suspension within the next six months, despite efforts by the current DSS leadership. As the Department of Defense comprises the bulk of requirements (in terms of numbers) for individuals with security clearances, the DSS dilemma is a stark indicator that the government's current personnel security process cannot meet today's needs. Certainly, a portion of the problem is that today's system is very labor-intensive and is completely out of step with today's demands in a highly information technology rich world. More importantly, the fundamental premise of today's process must change to better address today's society, the information environment within which this society exists, and the needs that the government, especially the Intelligence Community, has for engaging our society's rich cultural mix in order to have the best and brightest as part of the effort to protect our nation. Most importantly, today's process does not adequately meet today's threats, let alone those in the future. Therefore I implore the Committee to consider the larger picture and support the significant but necessary changes I have offered. Thank you.

Testimony of

Doug Wagoner

On behalf of the Security Clearance Reform Coalition

Before the Homeland Security and Government Affairs Committee
Of the U.S. Senate
May 17, 2007

Aerospace Industries Association
American Council of Engineering Companies
Armed Forces Communications & Electronics Association
Associated General Contractors of America
Association of Old Crows
Contract Services Association
Information Technology Association of America
Intelligence and National Security Alliance
National Defense Industrial Association
Professional Services Council

AIA
AEROSPACE INDUSTRIES ASSOCIATION

ACEC
AMERICAN COUNCIL OF ENGINEERING COMPANIES

AFCEA

THE ASSOCIATED GENERAL CONTRACTORS OF AMERICA
SKILL RESPONSIBILITY INTEGRITY

AOC

CSA
Contract Services Association
Excellence in Government Contracting

ITAA
Information Technology Association of America

INSA
INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

NDIA

PSC PROFESSIONAL SERVICES COUNCIL

SECURITY CLEARANCE REFORM COALITION
TESTIMONY BEFORE THE SENATE HOMELAND SECURITY AND GOVERNMENT AFFAIRS COMMITTEE
MAY 17, 2007

Good morning Mr. Chairman and Members of the Committee. My name is Doug Wagoner and I am the Chief Operating Officer of Sentrillion. I am speaking to you today as a member of the Information Technology Association of America (ITAA) and I would like to thank you for this opportunity and for your continued commitment to reforming the clearance granting process.

For the last several years, ITAA has led the Security Clearance Reform Coalition[1] of ten trade associations seeking to bring industry perspective and recommendations to the clearance granting process. Several of our previous recommendations were adopted as part of the 2004 Intelligence Reform and Terrorism Prevention Act (IRTPA). Just as this series of hearings has sought to do, we hope to monitor the clearance granting process and make recommendations to both the Administration and the Congress to bring relief from the significant problems this dysfunctional process causes for industry. My comments today will focus on the process as it relates to collateral DoD clearance applications, but we believe that all of government would benefit from the adoption and implementation of these suggestions. It must be noted that industry does not experience the same delays for clearances in the Intelligence Community and, in fact, most of that community is currently processing clearances within the metrics established in the IRTPA.

As I am sure you are aware, industry continues to face significant problems with the clearance granting process that result in a negative impact to our ability to meet the national and

[1] The Security Clearance Reform Coalition is comprised of the Aerospace Industries Association, the American Council of Engineering Companies, the Armed Forces Communications & Electronics Association, the Associated General Contractors of America, the Association of Old Crows, the Contract Services Association, the Information Technology Association of America, the Intelligence and National Security Alliance and the National Defense Industrial Association and the Professional Services Council. We represent hundreds of companies that provide thousands of cleared personnel to the departments and agencies of the U.S. government.

homeland security missions of the United States. Delays in processing persist because of the government's failure to adopt 21st century technology innovations; agencies which continue to craft their own requirements for mutual recognition of clearances; as well as a lack of prioritization at some departments and agencies coupled with funding mechanisms that prevent investment in cost and time-saving technologies. Our assessment of the status of the clearance granting process would not match the rosy picture painted in the Administration report to Congress this past February, but would more closely resemble the General Accountability Office (GAO) (GAO-06-1070) report as an accurate picture of conditions in the process.

Industry views the clearance granting process as having four distinct parts and we have adopted the mantra, "One application, one investigation, one adjudication and one clearance" to simply express our goals for improving the clearance granting process. Unfortunately, we do not believe that any of these goals have been achieved. To help bring about change and provide options for consideration by both the Congress and the Administration, you will find attached as an addendum to this testimony our latest set of recommendations for improvements. I would like to highlight one recommendation from each of the four sections of the process and point to the improvements that its adoption would bring.

APPLICATION

The single most critical improvement that *all* of government could adopt to improve the process would be the full and complete electronic application for a security clearance. As the stakeholders for the application stage of the process, collection and submission of the completed application package is the responsibility of the agency or department that provides a clearance for industry personnel. There are three parts to an application – a completed form SF-86, a signed release form and a complete set of the applicants' fingerprints. Industry applicants for the Department of Defense (DoD) now use the electronic questionnaire for investigative purposes, or e-QIP, to capture the SF-86, but the other components of the application package are either not collected electronically at all or they are collected using such antiquated techniques and technologies that they are a burden to the system instead of an improvement to the process.

Fingerprints are still collected and submitted using paper and ink fingerprint cards and manual rolling of the prints. This is baffling to industry, as all armed services' recruits have their fingerprints collected digitally at recruitment centers, the Department of Homeland Security has adopted digital fingerprint collection technologies for port workers and much of the nation's local law enforcement now use digital fingerprint technology for criminals. Industry has even offered to provide the necessary technology to submit digital fingerprints, but this offer has been declined because the databases are, apparently, incapable of accepting such digital submissions. This prevents the fingerprint cards from being bundled electronically with the application and the signature and instead requires that they must be separately packaged and mailed for later marriage with the electronic SF-86. As you can imagine, this creates significant opportunity for fingerprint cards to be lost or delayed in transit. An all too often result of this condition is that e-QIP applications are rejected for investigation because the fingerprint cards are not received in a timely fashion.

Signatures for applications at DoD are now collected electronically, but they are collected by the use of a facsimile machine, rather than the widely available technology now found on most checkout counters in America. This technologically antiquated signature collection method has created such a drain on the system resources of DoD's Joint Personnel Adjudication System (JPAS) that they have posted an apology on their website to their users for the processing delays. Furthermore, it has created a new, extremely negative condition in the application process described as "out of synch" applications. "Out of synch" applications are applications that are submitted using the e-QIP electronic form SF-86 and appear to have been successfully submitted to JPAS. In reality, these "out of synch" applications are instead lost in the digital ether and are never received. Currently, there are estimated to be over 2,000 industry applications that are "out of synch" and, potentially thousands of applications from the armed services that have been lost in the same fashion. "Out of synch" applications are not discovered until there is such a delay in the receipt of an interim clearance for the applicant that a knowledgeable industry security officer follows up and discovers the loss.

Industry would like to congratulate and support the efforts of the new Director of the Defense Security Service, Kathy Watson, for identifying these and other problems and making the corresponding suggestions for improvements to JPAS to correct them. We have been disappointed, however, in the lack of funding and prioritization at DoD that has prevented their expeditious resolution.

Implementation of this critical recommendation can occur immediately if the Office of Personnel Management (OPM) would simply enforce its' published requirement that all applications for investigation must be submitted electronically using e-QIP. This requirement was published almost two years ago, but OPM continues to receive and process between 25-40% of all applications in paper form. Large agencies, like the General Services Administration, also contribute to this problem by ignoring this requirement and requiring applicants to complete a paper copy of the 30-plus pages of the SF-86.

These inconsistent and disjointed application collection mechanisms that continue to rely upon manual submission of some or all of the components of the application create significant problems allowing the process to even get started. By eliminating any submission options except those using digital technologies, the application would be received, approved, and an investigation begun in a matter of minutes, instead of the weeks or even months inherent in the current process.

INVESTIGATION

The primary stakeholder for the investigation stage of the clearance process for over 90% of all clearances granted by the United States government is the OPM Federal Investigative Services Division or FISD. FISD is responsible for verifying receipt of a completed application from the agencies and departments and initiating an investigation corresponding to the level of clearance that is being requested.

Here, too, the process would greatly benefit from the adoption of 21st century technology to eliminate the tremendous amount of "touch labor" involved in the processing of applications at OPM. For example, clearance applications - even those submitted electronically - are printed out and a file folder much like one would encounter in a doctor's office with color-coded labels is created for each applicant. It is industry's opinion that it is this shuffling of the paper file, from clerks processing these files in the mine at Boyers, Pa., to the investigative personnel in the field and back again, and then finally on to the adjudicators that creates such a tremendous delay in the processing of clearances. Industry would recommend that government move to create and implement an end-to-end data management capability that begins with an electronic application created in e-QIP. During the investigative stage, that application would then be appended with relevant information obtained from commercial and government databases, such as credit histories and criminal records, and, finally, would be provided to the adjudicating agency as an interoperable electronic file with all relevant information readily available for adjudication. Instead, we currently have a process at FISD where electronically submitted information is printed out to create a hard-copy file, files are then mailed to investigators in the field for investigation, completed files are then tracked using manually affixed bar-coded labels and in many cases a hard copy summary is sent back to the originating agency for adjudication.

At the center of this tremendous amount of touch labor is the antiquated database dubbed PIPS or Personnel Investigations Processing System. This technology would have been abandoned and replaced decades ago in the private sector as out-of-date and a hindrance on efficiency. The system is completely isolated and does not share data directly with any other computer system in the application process. It would be impossible to make this system interoperable and to share data in real time in a cost efficient manner. Finally, the age of this system is prohibitive to the adoption and incorporation of most technological advances in information management from at least the last decade. As long as OPM continues to rely upon PIPS, there will be no way to eliminate the tremendous amount of touch labor in the investigative process, nor will it be possible to provide data in an end-to-end paperless fashion for the efficient application, investigation and adjudication of clearance applications. This disability also adversely impacts on the implementation of the reciprocal acceptance of clearances.

A final note must be made regarding the sharing of data both to and from FISD. OPM has frequently pointed to the "imaging" of data, like fingerprint cards and completed investigative files, as "automation" of the process. To be clear, imaging is not automation and does not necessarily contribute in any way to the efficiency of the process, but is simply the digital capture of a picture of a document. Without additional technology to read the image and extract the relevant data, imaging does nothing to improve the process and instead creates another step that clearance applications must undergo for processing.

ADJUDICATION

Accurate and reliable adjudicative outcomes can be improved through the receipt of complete cases from OPM to include full development and reporting of derogatory information in the course of the investigation. Currently, it is not unusual that, when relevant derogatory information is discovered, it is not fully explored, developed or mitigated in the investigative stage of the process, imposing enhanced and unnecessary risk assessment requirements on adjudicators. Some enhanced risk assessment requirements are necessary, for example in evaluating the trustworthiness of an applicant for translating services with ties or connections to countries in the Middle East that are listed as state-sponsors of terrorism. But intentionally leaving issues undeveloped, or labeling applications as "closed pending," abrogates responsibility for completion of the investigation and only exacerbates the condition, making it harder for adjudicators to accurately assess an applicant. Of course, industry also feels that adjudication would be significantly enhanced and made more efficient with the adoption of the end-to-end data sharing capability mentioned above.

RECIPROCITY

Bill Leonard at the Information Security Oversight Office and Clay Johnson at OMB should be applauded for their efforts to bring about the greater reciprocal acceptance of clearances across the federal government; but frequently their good intentions have been overcome by the intractability of old habits. This is in spite of the Congressional direction clearly provided in the IRTPA.

Trust in the adjudicative abilities of each agency, as well as the trustworthiness of the underlying investigative information used as the basis for the clearance, remains at the heart of the reciprocity issue. For example, empowering OPM as the single investigative source for the majority of the clearance needs of the government was a proper and correct step toward establishing uniformity and consistency in the process. Other steps, like the Central Intelligence Agency plan to enter unclassified clearance information into JPAS are applauded as enhancing the ability of agencies to verify clearances and should increase the trustworthiness of the data for users. But data sharing is still limited. While some agencies have indirect access to JPAS, as the sole system of record for collateral clearances for the

U.S. Government, all authorized agencies with a clearance granting mission should have direct and readily available access in order to give them the necessary tools to implement the reciprocity policies as intended.

Industry would ask Congress to reiterate and clarify their intentions included in the IRTPA regarding reciprocity to include the identification of agencies that are not in compliance with national reciprocity guidelines, and assign responsibility to compel those agencies to comply. Similar oversight should extend to the sharing of clearance data to verify the quality and completeness of clearance information being submitted to the existing clearance databases, namely JPAS and OPM's CVS. Without timely, accurate and reliable clearance information in a standardized, central database, reciprocity will continue to plague the clearance process with delays and unnecessary costs.

Industry would also ask Congress to clarify expectations regarding the implementation of Homeland Security Presidential Directive 12 (HSPD-12). HSPD-12 requires that all federal government employees and contractors accessing federal government facilities or information systems must be validated through a background investigation and issued an identification card attesting to the completion of such an investigation. Currently, it is not specified in law or regulation that the government is expected to accept as approved under the requirements of HSPD-12, without further need for investigation, all federal and contractor employees that currently hold a clearance. In order to prevent unnecessary and redundant investigations, and to reduce the workload on OPM FISD, as the identified entity responsible for investigations, we hope that this can be clarified.

BUDGET

On one final note, Congress must provide innovative and flexible budgetary authority to create a reliable and sufficient funding source for these agencies to undertake these and other improvements necessary for a world-class, end-to-end clearance system that will be in compliance with the IRTPA by December 2009. FISD, for example, receives no direct appropriations and instead must pay for their operations through fees assessed on their customers. As such, the federal government must develop a more accurate system for estimating the demand of industry and government clearances, and the appropriate agencies should submit budget requests that mirror the anticipated demand, with a limited reliance on premium charges.

Mr. Chairman, it is our sincere hope that these recommendations provide options for improving the clearance granting process. It is, however, but a start towards a much-needed re-evaluation and re-engineering of how the security clearance community does business in the 21st Century. We are ready and willing to discuss all of the recommendations we make in the addendum and look forward to working with you and the Committee to bring about additional improvements to the security of the United States through improvements to the clearance granting process.

SECURITY CLEARANCE REFORM COALITION
TESTIMONY BEFORE THE SENATE HOMELAND SECURITY AND GOVERNMENT AFFAIRS COMMITTEE
MAY 17, 2007

Recommendations of the Security Clearance Reform Coalition For Improvements to the Clearance Granting Process

Presented to the Homeland Security and Government Affairs Committee
Of the U.S. Senate
May 17, 2007

Aerospace Industries Association
American Council of Engineering Companies
Armed Forces Communications & Electronics Association
Associated General Contractors of America
Association of Old Crows
Contract Services Association
Information Technology Association of America
Intelligence and National Security Alliance
National Defense Industrial Association
Professional Services Council

AIA
AEROSPACE INDUSTRIES ASSOCIATION

ACEC
AMERICAN COUNCIL OF ENGINEERING COMPANIES

AFCEA

THE ASSOCIATED GENERAL CONTRACTORS OF AMERICA
SKILL RESPONSIBILITY INTEGRITY

AOC

CSA
Contract Services Association
Excellence in Government Contracting

ITAA
Information Technology Association of America

INSA
INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

NDIA

PSC
PROFESSIONAL
SERVICES
COUNCIL

These recommendations are focused on the collateral DoD clearance granting process, since many of the IC agencies are running efficient processes using state of the art technologies.

These recommendations are based upon extensive interviews with the various stakeholders in the clearance granting process to better understand what happens to an application as it moves through the process and are bolstered by the numbers of clearances in the backlog, defined as non-compliant with the metrics of the 2004 Intelligence Reform and Terrorism Prevention Act. These numbers as of mid-February, when 459,598* cases were reported in process, are:

- Initial Secret/Confidential: 113,161 over 90 days old with 81,680 "closed pending"
- Initial Top Secret: 45,185 over 90 days old with 7,566 "closed pending"
- Top Secret Reinvestigations: 39,925 over 180 days old with 10,786 "closed pending"
- All Others (suitability, etc.): 41,372 over 90 days old with 12,906 "closed pending"

TOTALS: 239,643 backlogged cases with 112,938 "closed pending" cases.* This amounts to 52% of all cases in process in the backlog and 48% of the backlogged cases categorized as "closed pending."

these totals DO NOT include secret/confidential reinvestigation numbers.

APPLICATIONS

1) <u>End-to-End Capability:</u> The process is one large paper shuffle and must adopt an end-to-end capability to share data interoperably in real-time. No such planning is currently underway, as there is no one manager for the process.

2) <u>Require Electronic Applications:</u> OPM must enforce the requirement published in the Federal Register requiring all new applications and renewals to be submitted via the Internet-based e-QIP. Currently, between 25-40% of all applications are still accepted in hard copy. Several major agencies, including the General Services Administration, still require applicants to complete paper applications and include other extraneous information, like resumes, as part of the application.

3) <u>Clarify Metrics:</u> Congress must clarify that the time frames established in the IRTPA for clearance processing begin when an application is actually received by the investigative agency, regardless of when it is actually scheduled. Frequently, the calendar for the investigation is not started until months after the application has been received by the investigative agency.

4) <u>Improve JPAS:</u> DoD must invest the funds necessary to make required improvements to JPAS. This is not happening at present and service is being degraded to the DoD adjudication facilities as well as to thousands of security managers in both government and industry who depend upon it for mission requirements. The JPAS user community and the Defense Security Service (DSS) have already identified the changes needed to

streamline and accelerate JPAS processing, but the level of priority for this problem seems to have fallen since last summer when DSS ran out of funding. These improvements include the ability to accept and capture digitized fingerprints and signatures from industry and eliminate delays and dropped applications caused by JPAS being out of synch.

INVESTIGATIONS

1) Modernize Data Capture: OPM must modernize its data capture procedures. Imaging, while frequently cited as an "automation" of the clearance process, is nothing more than taking a picture of a document and is ineffective at capturing the data in the document for use in an information technology system.
    a. OPM must stop accepting fingerprint cards and start using digitized fingerprint capture tools such as LiveScan.
    b. Signatures on release forms can also be easily captured using technology at checkout counters across America and eliminates the need to print and mail release forms to investigators when needed.
    c. Investigative files are also selectively imaged, where using truly digitized information would allow for the preservation of the entire file, not just summaries, and preserve critical information like credit reports and criminal histories.

2) Modernize Data Management at OPM: OPM-FISD continues to rely upon PIPS, an antiquated stand-alone mainframe computer system that is not interoperable and cannot be made so. This reliance forces continuation of labor-intensive paper handling that significantly delays the processing of clearances. Many of the problems identified by industry in the process are related to or stem from this reliance upon PIPS.
    a. PIPS does case assignment, but once a case is assigned, it is printed out and mailed to investigators for processing.
    b. For paperwork management, OPM relies upon barcodes, which are manually keyed, printed and affixed to documents in the hard copy files.
    c. Only some of the information collected during an investigation is preserved for future review or access by the adjudicators and other critical information sources, such as criminal and credit histories, are not retained.
    d. CVS is an important tool, but cannot adequately verify a clearance since it relies upon batched data and is not real-time.
    e. OPM must begin to share investigative results electronically. Currently, they do not share any investigation results electronically, but they do image some results. This does not facilitate adjudication processes, as none of the data can populate data management systems at the adjudicating agency.

3) Eliminate the "Closed Pending" status for clearances at OPM: OPM categorizes investigations that are incomplete due to the lack of some data or incomplete status of some component of the application as "closed pending." Some of these incomplete files are then passed to the originating agency for adjudication, while other departments, like DoD, refuse to accept or adjudicate these applications in "closed pending" status. Since this information is frequently needed to make adjudicative risk assessments, agencies

are then forced to return the application to OPM, thereby incurring further charges to process the clearance.

4) Implement the Use of Phased Periodic Reinvestigations (PR): The federal government should direct implementation of phased periodic reinvestigation (currently being implemented only by DoD) to realize the full benefits of scaling the PR in such a way that limits the use of costly and time consuming field investigation. Using commercial and government databases, cleared personnel are evaluated for any activity that would require further investigation (Phase I). If the Phase I results (automated checks and selected interviews) are favorable, there is no need to proceed to the costly field investigation (Phase II). Phased PR's can be conducted more frequently with less cost, so that the cleared personnel – those most in a position to cause harm to the United States – are more effectively monitored. It is conservatively estimated that such an approach could save 20% or more of the cost of conducting periodic reinvestigations.

5) Implement ACES or the Automated Continuing Evaluation System: ACES, by automatically checking a variety of government and commercial databases, can almost constantly monitor the activities of cleared personnel, daily checking them against government and commercial information sources for any activity that could require further investigation. This would facilitate and accelerate the government's ability to properly manage and monitor current clearance holders and to identify significant problems and issues of security concern whenever they occur, rather than on a periodic term (every 5-10 years). Any cases where issues are identified through ACES would undergo a full periodic reinvestigation. This approach would not only enhance security at a reasonable cost but would quickly provide a huge baseline of data to evaluate.

ADJUDICATIONS

1) Adequately Develop Derogatory Information: OPM has modified the criteria to which clearances at various levels are investigated, including dropping efforts to investigate and develop derogatory information for Secret collateral clearances. Such a change in the process makes it difficult if not impossible to effectively adjudicate many applications.

2) Enhance Training Standards: Develop and implement standardized professional training and certification criteria for adjudicators across the federal government. This would create equity in the training and development of adjudication officers and improve reciprocity of clearances by building trustworthiness across federal agencies with the application of adjudicative standards.

3) Establish Common Recordkeeping: Establish and implement a common approach across all agencies, using existing central clearance databases like CVS, JPAS, and Scattered Castles, for the recording of waivers, conditions, and deviations in order for adjudicators and security officers to have access to this information when taking an action to reciprocally accept another agency's clearance or access determination.

RECIPROCITY

1) Increase Clearance Data Sharing: Intelligence Community agencies should be required to populate JPAS with clearance/access information on non-classified employees. All such data should be validated to ensure that it is not corrupting critical, accurate information about existing clearance holders contained in the databases.

2) Reinforce Uniformity in the Application of Reciprocity: Some Intelligence Community agencies are requiring that a clearance must be "active" rather than "current" before it will be considered for acceptance under reciprocity rules. This approach necessitates obtaining the prior investigative file and re-adjudicating the clearance. This is a costly, time consuming and unnecessary process under existing policy and is in violation of the spirit, if not the letter, of the IRTPA. It is also in direct conflict with the provisions of EO 12968 and OMB memoranda of December 2005 and July 2006 (Checklist of Permitted Exceptions to Reciprocity) which require a valid "access eligibility determination."

3) Provide Access to JPAS for Authorized Agencies: All authorized Federal agencies should be given direct access to JPAS, as the sole system of record of the U.S. Government for all clearance and access eligibility determinations, in order to more fully and efficiently realize the goal of clearance/access reciprocity.

BUDGET AND PERSONNEL

1) Establish Efficient Budgetary Mechanisms: Budget issues were partly to blame for the processing moratorium on industry security clearances. As such, security clearance reform must include budget improvements as well. For instance, the federal government must develop a more accurate system for estimating the demand of industry clearances, and the appropriate agencies should submit budget requests that mirror the anticipated demand, with a limited reliance on charged premiums.

2) Enhance OPM Workforce Capabilities: Likewise, OPM's workforce capabilities must also be aligned to meet the anticipated demand for security clearances, as well as the demand for investigations of government and contractor personnel under HSPD-12 (industry estimates this requirement to include over 10M individuals). While some flexibility currently exists, industry is skeptical that it can meet these anticipated demands.

3) Build More Accountability Into the Invoicing Process for Clearances: OPM should not collect fees from the agency until the background check is completed and should provide greater clarity in their billing practices per the DoD IG investigation of these practices.

BACKGROUND
EVALUATING THE PROGRESS AND IDENTIFYING OBSTACLES IN IMPROVING THE FEDERAL GOVERNMENT'S SECURITY CLEARANCE PROCESS
MAY 17, 2007

BACKGROUND

The Department of Defense (DoD) is responsible for obtaining background checks on DoD military and civilian personnel, as well as DoD contract industry personnel. In addition, DoD provides clearances for legislative branch staff and has signed a memorandum of understanding with 23 federal agencies to do clearances for their industry personnel.

The number of clearance requests to DoD skyrocketed since the terrorist attacks of September 11, 2001. In 2005, the Government Accountability Office (GAO) placed the Department of Defense Security Clearance process on the GAO High Risk List due to a mounting backlog of clearance requests as well as DoD's inability to manage the backlog.

In February 2005, DoD transferred its investigative function as well as 1,800 investigative positions to the Office of Personnel Management's Federal Investigative Services Division (OPM/FISD). A total of 1,578 personnel were actually transferred. DoD now sends requests to OPM for investigation and the agency adjudicates the cases. However, many security clearances still take in excess of one year to complete[1].

INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004

In 2004 the President signed *the Intelligence Reform and Terrorism Prevention Act* (IRTPA) into law. This Act set several benchmarks aimed at improving the timeliness of the security personnel process, as well as other improvements to the process, including database management and reciprocity of clearances between agencies and departments. IRTPA set benchmarks for the investigative, adjudicative, and total times for clearances, as seen below.

IRTPA Benchmarks for Clearances
(Average Timeliness Required for 80% of Clearances)

Benchmark Date	Investigation	Adjudication	Total
by December 17, 2006	90 days	30 days	120 days
by December 17, 2009	40 days	20 days	60 days

On June 28, 2005, the President issued Executive Order 13381 in compliance with implementing IRTPA. E.O.13381 expired in 2006, but was extended through July 1, 2007. The order (1) designates the Office of Management and Budget (OMB) as the agency responsible for setting security clearance policy; (2) allows OMB to assign an agency to be in charge of conducting clearance investigations for the federal government (OMB chose OPM); (3) ensures reciprocity of clearances between agencies to more easily move employees from one agency to another; and (4) orders resources to be available and tools and techniques to be developed to enhance the security clearance process. Intelligence agencies who investigate their own cases

[1] GAO, *DOD Personnel Clearances: Additional OMB Actions are Needed to Improve the Security Clearance Processes*, GAO-06-1070, September 28, 2006.

must still comply with policies laid out in E.O.13381. The order did not alter the current process whereby some agencies are responsible for adjudicating their own clearances.

The IRTPA also mandated that OPM "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." OPM has established the Clearance Verification System (CVS), as a part of its Personnel Investigations Processing System (PIPS). However, DoD maintains their own separate database known as the Joint Personnel Adjudicative System (JPAS), which is accessible through PIPS via a secure connection to verify DoD clearances.

The DoD Security Clearance Process

In general, an agency requesting a security clearance forwards the case on to OPM for investigation. Cases are intiated with the subject filling out a Standard Form 86 (SF-86), or by filling out an online OPM form known as an Electronic Questionnaire for Investigations Processing (eQIP). This data is forwarded to investigators, who pull various records, including criminal and credit checks. Various other checks, including employment and residence verification take place, and some in-person investigation and field work is conducted.

If a case is deemed incomplete at OPM, it may be "closed pending," until the missing information can be gathered. A completed investigation is marked closed. After OPM has closes an investigation, they send the case file back to agencies for adjudication. When an agency has made a clearance determination, they are supposed to inform OPM of the individuals clearance status, which is tracked in the CVS through PIPS, unless it is a DoD clearance, in which case it is tracked in JPAS.

Clearance Processing Times

According to OMB in a report[2] required by IRTPA, all investigations completed by OPM after October 1, 2006, averaged 166 days, while all agency adjudications averaged 39 days, making the entire process average 205 days. OMB projects that the average time for <u>initial</u> requests for clearance begun after October 1, 2006, will be in line with the IRTPA goal of 120 days or less. In contrast, most intelligence community clearances, which are not handled by OPM, are completed much more quickly.

GAO last issued a report[3] on the Security Clearance Process in September 2006. The report found that investigative and adjudicative times had decreased, but that data provided by OPM may not be accurate. GAO's analysis of OPM and OMB data showed that on average, initial investigations took 286 days and adjudications took 39 days for top secret investigations. It should be noted that top secret investigations take considerably longer in general than a confidential or secret investigation.

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

[3] GAO, *DOD Personnel Clearances: Additional OMB Actions are Needed to Improve the Security Clearance Processes*, GAO-06-1070, September 28, 2006.

There is also time involved in the agency submitting a security clearance request to OPM. According to the same GAO report, in FY2006, it took agencies an average of 30 days to submit hardcopy security clearance requests to OPM, though only 15 days to submit electronically through OPM's eQIP. OPM's goal for submittal is 14 days and for all agencies to submit 100% of requests through eQIP. GAO found that it took an average of 111 days for agencies to submit an initial top secret clearance.

THE DEFENSE SECURITY SERVICE

By far, most security clearance requests are made through the Defense Security Service (DSS). Last April, DSS, which processes all security clearance applications from contractors for the DoD and 23 other federal agencies, halted security clearance processing for all contract personnel. At the time, DSS blamed the sheer volume of requests and a budget shortfall. DSS pays OPM on a per-investigation basis for clearances.

DSS has frequently been cited by GAO[4] for an inability to accurately estimate its workload, which creates a budgetary problem for DSS and a staffing problem for OPM. DSS received a budgetary fix last year and restarted clearance submittals. In FY2006, DoD's workload estimate was off by more than 5 percent[5].

TECHNOLOGY

Various pieces of technology contribute to the process of security clearances. A brief description of the major computer systems involved follow.

DoD - Joint Personnel Adjudication System (JPAS)[6]

DoD maintains its own adjudication and clearance tracking system since, known as JPAS. JPAS was envisioned to be a repository for adjudication information, but now performs many other functions, such as electronically processing faxed information related to the adjudication and clearance process.

JPAS has increasingly experienced system problems, which are most likely attributed to the piece-meal nature in which it has been developed over the past several years. On April 28, 2007, JPAS had to be taken down for 12 hours to perform system maintenance.

OPM - Clearance Verification System (CVS)[7]

The IRTPA required that a centralized database for maintaining clearance information be maintained by OPM. OPM tailored CVS to serve as this database. Agencies can access the CVS, via PIPS, to check on the clearance verification of an individual.

[4] GAO, *DOD Personnel Clearances: Additional OMB Actions are Needed to Improve the Security Clearance Processes*, GAO-06-1070, September 28, 2006.

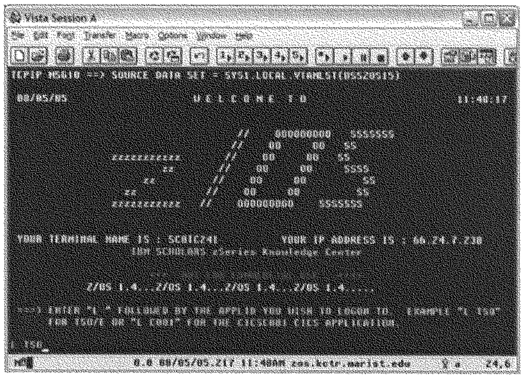
[5] OMB, *Report of the Security Clearance Oversight Group Consistent with Title III of the Intelligence Reform and Terrorism Prevention Act of 2004*, February 2007, Agency Performance Report Chart.

[6] DoD JPAS Website, https://jpas.dsis.dod.mil/

[7] OPM, *Use of Information Technology in OPM Background Investigations*, February 2006

OPM – Personnel Investigation Processing System (PIPS)[8]

OPM uses its own database developed in 1984, known as the Personnel Investigation Processing System. PIPS is housed on an IBM z/900 mainframe running the z/OS operating system. z/OS systems are accessed using a terminal program. A standard z/OS terminal screen is below, similar to what those accessing the PIPS system would experience. Most commands are keyboard based rather than using a mouse.



```
TCPIP MSG10 ==> SOURCE DATA SET = SYS1.LOCAL.VTAMLST(USSZOS15)

 08/05/05                    W E L C O M E   T O                         11:40:17

                                      //    000000000    SSSSSSS
                                     //    00      00   SS
                   zzzzzzzzzz       //    00      00   SS
                           zz      //    00      00     SSSS
                        zz        //    00      00         SS
                     zz          //    00      00         SS
                   zzzzzzzzzz   //    000000000    SSSSSSS


 YOUR TERMINAL NAME IS : SC0TC241          YOUR IP ADDRESS IS : 66.24.7.230
                       IBM SCHOLARS zSeries Knowledge Center


          Z/OS 1.4...Z/OS 1.4...Z/OS 1.4...Z/OS 1.4.....

 ===> ENTER "L " FOLLOWED BY THE APPLID YOU WISH TO LOGON TO.  EXAMPLE "L TSO"
      FOR TSO/E OR "L C001" FOR THE CICSC001 CICS APPLICATION.

L TSO_
 MA          0.0 08/05/05.217 11:40AM zos.kctr.marist.edu                 24,6
```

http://www-304.ibm.com/jct09002c/university/students/contests/mainframestudents_part1.html

The text-based PIPS system has had numerous enhancements since its introduction, when it only housed OPM's Security/Suitability Investigations Index. It has now expanded to include automated scheduling, tracking, control, and closing of investigations. PIPS is now also electronically connected with the various National Agency Checks. PIPS also includes automated case billing, penlight tracking of bar-coded investigation materials, and reporting.

A PIPS reporting function was also added to better communicate with field investigators. With the increased demand for electronic imaging of data, and for OPM to comply with various federal electronic mandates, OPM added a PIPS imaging system which can scan and print several pieces of investigations and materials.

OPM – Electronic Questionnaire for Personnel Investigations (eQIP)[9]

As stated earlier, eQIP is an electronic version of the Standard Form 86 (SF-86) which it is encouraging all applicants to file for investigations. eQIP is a web interface which can interactively question applicants, minimizing errors in data submission that are inherent with filling out a paper form. This data is then automatically entered into the PIPS system. Hard

[8] OPM, *Use of Information Technology in OPM Background Investigations*, February 2006

[9] OPM eQIP Website, http://www.opm.gov/e-qip/faq.asp

copies submitted to OPM are keyed into PIPS twice to ensure accuracy, though it also slows down the process.

ADDITIONAL INFORMATION/RESOURCES:

Government Accountability Office, *DOD Personnel Clearances: Additional OMB Actions are Needed to Improve the Security Clearance Processes*, GAO-06-1070, September 28, 2006. [http://www.gao.gov/new.items/d061070.pdf]

Office of Management and Budget, *Report of the Security Clearance Oversight Group Consistent with Title III of the Intelligence Reform and Terrorism Prevention Act of 2004*, February 2007. [http://www.whitehouse.gov/omb/pubpress/2007/sc_report_to_congress.pdf]

Office of Personnel Management, *Use of Information Technology in OPM Background Investigations*, February 2006. [http://www.ncms-valleyofsun.org/ncms/OPM%20Technology%20Report%20-%20Security%20Clearances%20-%202006.pdf]

Office of Personnel Management, *Fiscal Year 2006 Performance and Accountability Report – Part D*, April 20, 2005. [http://www.opm.gov/gpra/opmgpra/par2006/index.asp]

Defense Security Service, *Joint Personnel Adjudication System (JPAS): The "How-To" Book for Joint Clearance & Access Verification System (JCAVS).* June 2004. [http://www.dss.mil/diss/jpas/docs/JPAS-How-to-Manual.pdf]

DHS Office of the Inspector General, *Major Management Challenges Facing the Department of Homeland Security*, OIG-06-14, December 2006. [http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_07-12_Dec06.pdf]

HSGAC/ OGM Hearing, *Progress or More Problems: Assessing The Federal Government's Security Clearance Process*, S. Hrg. 109-621. May 17, 2006

HSGAC/ OGM Hearing, *Access Delayed: Fixing The Security Clearance Process,* S. Hrg. 109–160. June 28, 2005.

HSGAC/ OGM Hearing, *Access Delayed: Fixing The Security Clearance Process—Part II,* S. Hrg. 109–581. November 9, 2005.

LEGISLATION AND EXECUTIVE ORDERS

Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638. EO 13381 as amended by EO 13408, "Strengthening Processes Relating to Determining Eligibility for Access to Classified National Security Information".