AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

WHAT'S THE HOLD UP? A REVIEW OF SECURITY CLEARANCE BACKLOG AND RECIPROCITY ISSUES PLAGUING TODAY'S GOVERNMENT AND PRIVATE SECTOR WORKFORCE

HEARING

BEFORE THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

MAY 6, 2004

Serial No. 108–199

Printed for the use of the Committee on Government Reform



Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

95–869 PDF WASHINGTON : 2004

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENT REFORM

TOM DAVIS, Virginia, *Chairman*

DAN BURTON, Indiana
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
JOHN L. MICA, Florida
MARK E. SOUDER, Indiana
STEVEN C. LATOURETTE, Ohio
DOUG OSE, California
RON LEWIS, Kentucky
JO ANN DAVIS, Virginia
TODD RUSSELL PLATTS, Pennsylvania
CHRIS CANNON, Utah
ADAM H. PUTNAM, Florida
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, JR., Tennessee
NATHAN DEAL, Georgia
CANDICE S. MILLER, Michigan
TIM MURPHY, Pennsylvania
MICHAEL R. TURNER, Ohio
JOHN R. CARTER, Texas
MARSHA BLACKBURN, Tennessee
PATRICK J. TIBERI, Ohio
KATHERINE HARRIS, Florida

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
CHRIS VAN HOLLEN, Maryland
LINDA T. SANCHEZ, California
C.A. "DUTCH" RUPPERSBERGER, Maryland
ELEANOR HOLMES NORTON, District of Columbia
JIM COOPER, Tennessee

BERNARD SANDERS, Vermont
(Independent)

MELISSA WOJCIAK, *Staff Director*
DAVID MARIN, *Deputy Staff Director/Communications Director*
ROB BORDEN, *Parliamentarian*
TERESA AUSTIN, *Chief Clerk*
PHIL BARNETT, *Minority Chief of Staff/Chief Counsel*

CONTENTS

Page

Hearing held on May 6, 2004 1

Statement of:

Shenoy, Sudhakar V., chairman, Northern Virginia Technology Council; Bobbie G. Kilberg, president, Northern Virginia Technology Council, accompanied by Gary Nakamoto, NVTC; and Douglas Wagoner, chairman, Intelligence and Security Task Group, Information Technology Association of America 83

Wilshusen, Gregory C., Acting Director, Defense Capabilities and Management, U.S. General Accounting Office; Stephen C. Benowitz, Associate Director, Division for Human Resources Products and Services, U.S. Office of Personnel Management; Heather Anderson, Acting Director of Security, Office of the Under Secretary of Defense for Intelligence; and J. William Leonard, Director, Information Security Oversight Office 12

Letters, statements, etc., submitted for the record by:

Anderson, Heather, Acting Director of Security, Office of the Under Secretary of Defense for Intelligence, prepared statement of 50

Benowitz, Stephen C., Associate Director, Division for Human Resources Products and Services, U.S. Office of Personnel Management, prepared statement of 43

Davis, Chairman Tom, a Representative in Congress from the State of Virginia, prepared statement of 4

Leonard, J. William, Director, Information Security Oversight Office, prepared statement of 63

Shenoy, Sudhakar V., chairman, Northern Virginia Technology Council, prepared statement of 85

Wagoner, Douglas, chairman, Intelligence and Security Task Group, Information Technology Association of America, prepared statement of 120

Waxman, Hon. Henry A., a Representative in Congress from the State of California, prepared statement of 8

Wilshusen, Gregory C., Acting Director, Defense Capabilities and Management, U.S. General Accounting Office, prepared statement of 15

WHAT'S THE HOLD UP? A REVIEW OF SECURITY CLEARANCE BACKLOG AND RECIPROCITY ISSUES PLAGUING TODAY'S GOVERNMENT AND PRIVATE SECTOR WORKFORCE

THURSDAY, MAY 6, 2004

HOUSE OF REPRESENTATIVES,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The committee met, pursuant to notice, at 10:24 a.m., in room 2154, Rayburn House Office Building, Hon. Tom Davis of Virginia (chairman of the committee) presiding.

Present: Representatives Tom Davis of Virginia, Platts, Schrock, Miller, Blackburn, Waxman, Maloney, Cummings, Tierney, Clay, Watson, Van Hollen, and Norton.

Also present: Representative Moran of Virginia.

Staff present: David Marin, deputy staff director and director of communications; Ellen Brown, legislative director and senior policy counsel; Robert Borden, counsel and parliamentarian; John Cuaderes, senior professional staff member; Mason Alinger, professional staff member; Teresa Austin, chief clerk; Brien Beattie, deputy clerk; Jason Chung, legislative assistant; Kristin Amerling, minority deputy chief counsel; Earley Green, minority chief clerk; Jean Gosa, minority assistant clerk; and Andrew Su, minority professional staff member.

Chairman TOM DAVIS. Good morning. A quorum being present, the Committee on Government Reform will come to order.

I want to welcome everybody to today's hearing on the issues surrounding the Federal Government's ability to issue security clearances in a timely manner. This hearing continues the committee's review of personnel security clearance processing and reciprocity. I want to thank Chairman Shays and his staff for their work on this issue.

Today we are concentrating on clearances granted to the defense contractor community and how delays in the process cause major inefficiencies, which eventually lead to higher costs for taxpayers and ultimately harms national security. This hearing will also delve into the issue of reciprocity, more specifically, how despite Executive orders and Presidential directives mandating reciprocity, turf battles and trust issues have plagued our Government's agencies, resulting in delays and contributing to the overall backlog.

As a result of the terrorist attacks of September 11, 2001, the country has increased the awareness of threats to our national se-

curity. We have developed new programs, new technologies, and even new government agencies to deal with the threats appropriately. It is not surprising, then, that the demand for security clearances for both Government employees and industry personnel has dramatically increased over the last few years. Unfortunately, the Government mechanisms that investigate and adjudicate personnel security clearances have not caught up with the necessity to process security clearance requests for industry personnel quickly and efficiently. Industry personnel face additional challenges once they have a security clearance from one agency but then need to work on a project on behalf of a different agency. Often agencies do not recognize clearances granted by their sister agencies and therefore require industry personnel to go through the security process once again, which contributes more to the backlog.

As a result, many defense contractor companies are unable to hire otherwise qualified employees because the security clearance process is requiring, on average, over a year to complete, with all signs pointing to continued increases if something does not change. Defense contractor companies often rely on hiring, almost at a premium already cleared employees from other firms, thus increasing contract costs, which are then passed on to the taxpayer. Ultimately, these backlogs hurt national security. When industry employees are hired to work in security programs but cannot work on projects while they are waiting to be cleared, the contracts are not being completed and national security is jeopardized.

The security clearance process is composed of four parts: pre-investigation, initial investigation, adjudication, and periodic reinvestigation. The General Accounting Office, Department of Defense, Office of Personnel Management, and the private sector all agree that there are serious problems in each of these stages. As of the end of March 2004, DOD has identified roughly 188,000 backlog cases affecting contractors. To put this number into proper context, DOD has stated that the number of overdue requests for reinvestigations of clearances is unknown, and was believed to have grown from 300,000 in 1986 to 500,000 in 2000.

DOD's performance for completing the security clearance process is 75 days for an initial secret clearance, 120 days for an initial top secret, and 180 days for a reinvestigation of a top secret clearance. Yet in fiscal year 2003, on average, it took 375 days for a security clearance to make its way through the whole process. So let me be blunt: 375 days for a security clearance is unacceptable, and I am hoping that today we will all agree on a solution, or solutions, not only to reduce the backlog but also to process clearances efficiently and effectively from here on out.

To a certain extent, the backlog is caused by a human capital shortage in the investigation state of the process. In an effort to improve the security clearance issuing process, in November 2003, Congress authorized a proposed transfer of DOD's personnel security investigative functions and more than 1,800 investigative employees to the Office of Personnel Management [OPM]. To date, this transfer has not occurred, and it is my understanding that an even larger backlog is developing because this hand-off has not been completed. I hope that by the end of the day this committee will get some concrete answers as to why the transfer has not

taken place, and even more importantly when it is going to occur. I hope more than a mere interagency disagreement is to blame.

There are other ways to reduce our backlog shortage. In many ways the clearance process is still highly dependent on an outdated system in which paper shuffling is still king. We need to bring this process into the 21st century. An effective, all-encompassing, electronic system which allows for seamless information collection and extraction will go a long way in reducing backlog and, more importantly, reducing the time it takes to get a security clearance. I understand that DOD and OPM have on their plates aggressive plans to get us away from a paper driven process to one that is electronically accessible. This last Monday, OPM announced the progress it has made in the programs supporting the e-Clearance initiative. I am hopeful the witnesses here today can expand on these programs and tell this committee when we will see the seamless automation of information gathering and sharing promised under the initiative.

Finally, the committee is aware that the lack of true reciprocity is a major factor in the backlog. For agencies to deny a transfer just because of turf issues is just inexcusable. The mandate from the 1995 Executive Order 12968 that background investigations and eligibility determinations would be mutually and reciprocally accepted by all agencies needs to be strictly enforced, and since it is not, perhaps legislation mandating reciprocity should be in the offing.

Throughout this hearing we will also hear proposals for improvements, not just from the agencies but from our private sector witnesses as well. We should take heed of these suggestions, and if they make sense we should embrace them.

Through this hearing, the committee hopes to learn about the processes that are in place to alleviate some of the backlog the system now faces. Furthermore, what standards are in place where reciprocity may be granted across Federal agencies? What metrics exist to measure an agency's compliance with reciprocity requirements? What are DOD and OPM doing to ensure that clearances are granted in a timely manner? What measures have they planned under the e-Government Initiatives to provide for reciprocity and a reduction of the backlog? What communication is taking place between industry and Government to provide for a better understanding of these issues? The committee also hopes to learn what policy guidance is needed from the administration in order to provide for reciprocity and cohesiveness between agencies.

We have two impressive panels of witnesses before us to help us understand the issues surrounding the backlog of security clearances. First, we are going to hear from the General Accounting Office, followed by the Office of Personnel Management, and then the Department of Defense and the Information Security Oversight Office. We will then hear from our second panel of witnesses, representing the Northern Virginia Technology Council, and the Information Technology Association of America. I want to thank all of our witnesses for appearing before the committee. I look forward to their testimony.

[The prepared statement of Chairman Tom Davis follows:]

Opening Statement
Chairman Tom Davis
Committee on Government Reform
"What's the Hold Up? A Review of Security Clearance Backlog and Reciprocity Issues Plaguing Today's Government and Private Sector Workforce"
May 6, 2004

I would like to welcome everyone to today's hearing on the issues surrounding the Federal government's ability to issue security clearances in a timely manner. This hearing continues the Committee's review of personnel security clearance processing and reciprocity. I would like to thank Chairman Shays and his staff for their work on this issue. Today we are concentrating on clearances granted to the defense contractor community and how delays in the process cause major inefficiencies, which eventually leads to higher costs for the taxpayer and ultimately harms national security. This hearing will also delve into the issue of reciprocity -- more specifically, how despite executive orders and presidential directives mandating reciprocity, turf battles and trust issues have plagued our government's agencies, resulting in delays and contributing to the overall backlog.

As a result of the terrorist attacks of September 11, 2001, the country has increased the awareness of threats to our national security. We have developed new programs, new technologies, and even new government agencies to deal with the threats appropriately. It is not surprising, then, that the demand for security clearances for both government employees and industry personnel has dramatically increased over the last few years. Unfortunately, the government mechanisms that investigate and adjudicate personnel security clearances have not caught up with the necessity to process security clearance requests for industry personnel quickly and efficiently. Industry personnel face additional challenges once they have a security clearance from one agency but then need to work on a project on behalf of a different agency. Often agencies do not recognize clearances granted by their sister agencies and therefore require industry personnel to go through the security clearance process yet again.

As a result, many defense contractor companies are unable to hire otherwise qualified employees because the security clearance process is requiring, on average, over a year to complete, with all signs pointing to continued increases if something isn't done. Defense contractor companies often rely on hiring, almost always at a premium, already cleared employees from other firms, thus increasing contract costs, which are then passed on to the taxpayer. Ultimately, these backlogs hurt national security. When industry employees are hired to work in security programs but cannot work on projects while they are waiting to be cleared, the contracts are not being completed and national security is jeopardized.

The security clearance process is composed of four parts: pre-investigation, initial investigation, adjudication, and periodic reinvestigation. The General Accounting Office, Department of Defense, Office of Personnel Management, and the private sector all agree that there are serious problems in each of these stages. As of the end of March 2004, DOD has identified roughly 188,000 backlog cases affecting contractors. To put this number into proper

context, DOD has stated that the number of overdue requests for reinvestigations of clearances is unknown, and was believed to have grown from 300,000 in 1986 to 500,000 in 2000.

DOD's performance standard for completing security the clearance process is 75 days for an initial secret clearance, 120 days for an initial top secret, and 180 days for a reinvestigation of a top-secret clearance. Yet in fiscal year 2003 it took, on average, 375 days for a security clearance to make it through the whole process. Let me be blunt: 375 days for a security clearance is unacceptable, and I am hoping that today we will all agree on a solution, or solutions, not only to reduce the backlog but also to process clearances efficiently and effectively from here on out.

To a certain extent, the backlog is caused by a human capital shortage in the investigation stage of the process. In an effort to improve the security clearance issuing process, in November of 2003, Congress authorized a proposed transfer of DOD's personnel security investigative functions and more than 1,800 investigative employees to the Office of Personnel Management (OPM). To date this transfer has not occurred, and it is my understanding that an even larger backlog is developing because this hand-off has yet to be completed. I hope that by the end of the day this Committee will get some concrete answers to why the transfer hasn't taken place, and even more importantly when it will occur. I hope more than a mere interagency disagreement is to blame.

There are other ways to reduce our backlog shortage. In many ways the clearance process is still highly dependent on an outdated system in which paper shuffling is still king. We need to bring this process into the 21st Century. An effective, all-encompassing, electronic system which allows for seamless information collection and extraction will go a long way in reducing backlog and, more importantly, reducing the time it takes to get a security clearance. I understand that DOD and OPM have on their plates aggressive plans to get us away from a paper driven process to one that is electronically accessible. On May 3, OPM announced the progress it has made in the programs supporting the e-Clearance initiative, and I am hopeful that the witnesses here today can expand on these programs and tell this Committee when we will see the seamless automation of information gathering and sharing promised under the initiative.

Finally, the Committee is aware that the lack of true reciprocity is a major factor in the backlog. For agencies to deny a transfer just because of "turf" issues is inexcusable. The mandate from the 1995 Executive Order 12968 that background investigations and eligibility determinations would be mutually and reciprocally accepted by all agencies needs to be strictly enforced, and since it isn't, perhaps legislation mandating reciprocity should be in the offing.

Throughout this hearing we will also hear proposals for improvements, not just from the agencies but from our private sector witnesses as well. We should take heed of these suggestions, and if they make sense we should embrace them.

Through this hearing, the Committee hopes to learn about what processes are in place to alleviate some of the backlog the system now faces. Furthermore, what standards are in place where reciprocity may be granted across federal agencies? What metrics exist to measure an agency's compliance with reciprocity requirements? What are DOD and OPM doing to ensure

that clearances are granted in a timely manner? What measures have they planned under the e-Gov Initiatives to provide for reciprocity and a reduction of the backlog? What communication is taking place between industry and government to provide for a better understanding on these issues? The Committee also hopes to learn what policy guidance is needed from the Administration in order to provide for reciprocity and cohesiveness between agencies.

Chairman TOM DAVIS. I ask unanimous consent that Representative Moran be allowed to sit and ask questions of the panel. And without objection, so ordered.

I now yield to the Ranking Member, Mr. Waxman.

Mr. WAXMAN. Thank you, Mr. Chairman. I am pleased you are holding this hearing. Like you, I am concerned about the increasing backlog in processing security clearance requests and I want our committee to continue to focus on this issue.

An effective security clearance system is integral to our national security. We need a sufficient pool of individuals who can carry out the research, investigations, and other myriad tasks necessary to protect our citizens, and we need to know that security clearances are up to date so we can be confident that untrustworthy individuals cannot access our Nation's sensitive information. That is why the tremendous backlog regarding the processing of security clearance applications and renewals is so troubling. Qualified applicants, whether they are civil servants, service members, or industry contractors, should not have to wait over a year to obtain the necessary clearance to start their work. Yet, that is exactly where we stand today. The estimated backlog of security clearances is hundreds of thousands of applications, and this is simply unacceptable.

I look forward to learning more about how we can address this problem from today's hearing and working with you and our colleagues on this committee so that we can change the situation.

[The prepared statement of Hon. Henry A. Waxman follows:]

Statement of Rep. Henry A. Waxman, Ranking Minority Member
Committee on Government Reform
Hearing on
"What's the Hold Up? A Review of Security Clearance Backlog and Reciprocity Issues Plaguing Today's Government and Private Sector Workforce"
May 6, 2004

Mr. Chairman, thank you for holding this hearing. Like you, I am concerned about the increasing backlog in processing security clearance requests, and I am pleased that the Committee continues to focus on this issue.

An effective security clearance system is integral to our national security. We need a sufficient pool of individuals who can carry out the research, investigations, and other myriad tasks necessary to protect our citizens. And we need to know that security clearances are up to date so we can be confident that untrustworthy individuals cannot access our nation's sensitive information.

That is why the tremendous backlog regarding the processing of security clearance applications and renewals is so troubling. Qualified applicants, whether they are civil servants, service members, or industry contractors, should not have to wait over a year to obtain the necessary clearance to start their work -- yet that is exactly where we stand today.

The estimated backlog of security clearances is hundreds of thousands of applications. This is simply unacceptable.

I look forward to learning more about how we can address this problem in today's hearing.

Chairman TOM DAVIS. Thank you very much. Any other Members wish to make opening statements? Mr. Schrock.

Mr. SCHROCK. Mr. Chairman, I can do it now or I can wait until the time comes, although if it takes my time I would rather do it now.

Chairman TOM DAVIS. Go ahead.

Mr. SCHROCK. OK. Thanks, Mr. Chairman, for holding this hearing. This is a topic I hear a lot about with the folks that I represent in the Hampton Roads area of Virginia. Let me thank the witnesses for coming here today and helping us address and improve a program that is really quite vital to our national security. In today's world, I am hard pressed to think of any issue more important than ensuring that our national secrets are protected and shared with only those citizens who truly have a need to know and who are vetted as trustworthy.

In my naval career I was frequently confronted by the issue of security clearances and have seen many improvements in programs over the years. I recall once upon a time when a full scope investigation required that every interview be conducted in person and that each and every reported investigation included long narrations of each interview. Such a report was reviewed by an adjudicator who then made clearance recommendations based upon what was referred to as the "whole person" concept. The process, understandably, was lengthy, manpower intensive, and time consuming. Today's investigations have been significantly streamlined and reports, unless derogatory issues surface, are brief and to the point. The investigative process has been expedited and in many cases reference interviews can be conducted over the telephone.

The age of computers is here and so much more can be done, and should be done, electronically. This fact, too, should be contributing to an expedited security clearance process. It stands to reason that the investigative process should be considerably shorter than in the past, yet I am confounded to hear that an average investigation can now exceed a full year.

We in Congress have a duty to ensure our Federal expenses are appropriate and getting us the best return on our dollar. National security should not be compromised as a function of saving money. However, we are duty bound to oversee that the executive agencies are wisely spending such funds and providing the taxpayer the best return on investment. Such cases as Ames, Nicholson, and Hansen of only a few years ago are daily reminders of the importance of the security clearance process and we must ensure the integrity is fully integrated into that process.

I had the occasion to speak at length with a former Defense Investigative Service agent about this matter. I had some deficits in the program brought to my attention. Probably the greatest was the accountability of the field agents to produce. While all sorts of statistics relative to productivity are maintained, rarely are field agents admonished in a meaningful way for lack of productivity, and similarly, nor are their supervisors. While I would never encourage statistics to be the lone factor in the investigative process, recognizing that more difficult or, as they are called, derogatory cases take considerably more time, field agents need to be held accountable for their productivity. Continued Federal employment

and, indeed, our national security which suffers as a result of backlog investigations should depend on it. I expect that the witnesses would agree with me. And when my time comes I will have several questions. Thank you, Mr. Chairman.

Chairman TOM DAVIS. Thank you very much. Any Members wish to make statements? Mr. Moran.

Mr. MORAN. Thank you very much, Mr. Chairman, and thank you for once again bringing to light an issue that desperately needs to be addressed. I think we have a crisis situation here and it is a national security issue because we have such a backlog. We have heard from a great many new and innovative firms that have services that are undoubtedly invaluable to the Federal Government, but they are getting benched because it is going to take up to a year to be cleared for security reasons. We were notified last month that DOD has a backlog of 188,000 cases for defense industry personnel. As a result, things have bogged down and it is hurting us in the field in any number of areas.

As the chairman knows, I am on the Defense Appropriations Subcommittee and, as DOD knows, they have not asked us for any personnel to fix the situation. Here we are told that you wants to contract out basically to OPM to do the investigative process. But that is going to take more than a year before that transfer is completed. We do not know what the cost is going to be. We do not even know that OPM is going to be able to do it more efficiently and effectively. We have another appropriations hearing today. I want to find out why you have not asked for the people that could have relieved this backlog when it really has substantially affected the ability of DOD to carry out its mission. Thank you, Mr. Chairman.

Chairman TOM DAVIS. Thank you. Any other Members wish to make statements? Ms. Watson.

Ms. WATSON. Thank you so much, Mr. Chairman. I, too, must join with my colleague. We are hearing that there is going to be a request for anywhere from $25 billion to $50 billion for Iraq. I am wondering if there is some way we can put into that appropriation money for security, not only there but here as well. As I read the analysis in front of us, it says that defense contract companies are unable to hire. And the contractors—and I have a question about them which I will raise later—but we need to be sure that we are contracting with people with integrity, people with character, and so on. It takes time. It takes money. And so I am going to ask as you make your presentations, if there are proposals for additional funding so that we can have the man and woman power to be able to staff the security sites adequately.

I want to thank you, Mr. Chairman, for holding this hearing. Now is the time, and what is the hold up? Thank you.

Chairman TOM DAVIS. Thank you. Mr. Van Hollen.

Mr. VAN HOLLEN. Thank you, Mr. Chairman. Thank you for holding this hearing because I, too, am hearing from lots of people in my district on this issue, and not just from the contracting community, but also people who are working in the administration. I do think that we are seeing lots of initiatives designed to protect our homeland security, to protect our defenses being stalled as a result of this backlog.

It is kind of a strange irony that the security clearance process and the backlogs in the security clearance process would actually be hindering our efforts to enhance the security of our country. And again, we are hearing not just from people and companies who have innovative ideas, but also from representatives from the U.S. Government, Department of Defense, Department of Homeland Security, who want to engage these contractors and they are experiencing this terrible backlog with security clearances. So it seems to me the answer, obviously, is not to shortcut the security clearance process or to change those standards, but the obvious answer is to put the resources that we need into getting this done.

I just want to thank the chairman and my other colleagues here for moving ahead on this issue, because every day that the backlog grows is a day that important initiatives to protect homeland security go unmet. Thank you.

Chairman TOM DAVIS. Thank you very much.

We now move to our first panel of witnesses. I want to thank Gregory Wilshusen, Acting Director of Defense Capabilities and Management, U.S. General Accounting Office; Stephen Benowitz, the Associate Director of the Division for Human Resources Products and Services, U.S. Office of Personnel Management; Heather Anderson, Acting Director of Security, Office of the Under Secretary of Defense for Intelligence; and J. William Leonard, Director, Information Security Oversight Office, for taking time from their busy schedules to be here today. It is a policy of this committee that all witnesses be sworn before you testify. So if you would rise and raise your right hands.

[Witnesses sworn.]

Chairman TOM DAVIS. Let me just identify Mr. Wilshusen from GAO has brought a couple of assistants.

Mr. WILSHUSEN. Mark Pross and Jack Edwards.

Chairman TOM DAVIS. OK. Mark Pross and Jack Edwards have taken the oath, too. Thank you very much.

The rules of the committee is your entire testimony is part of the record and questions will be based on that. You have a clock of sorts in front of you, when it is green, it is go; when it is yellow, it means that 4 minutes are up, when it is red it means 5 minutes are up, and if you could move to summary as you get the red light things could move expeditiously. Again, thank you all for being with us.

Mr. Wilshusen, we will start with you and move straight down the table.

STATEMENTS OF GREGORY C. WILSHUSEN, ACTING DIRECTOR, DEFENSE CAPABILITIES AND MANAGEMENT, U.S. GENERAL ACCOUNTING OFFICE; STEPHEN C. BENOWITZ, ASSOCIATE DIRECTOR, DIVISION FOR HUMAN RESOURCES PRODUCTS AND SERVICES, U.S. OFFICE OF PERSONNEL MANAGEMENT; HEATHER ANDERSON, ACTING DIRECTOR OF SECURITY, OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE; AND J. WILLIAM LEONARD, DIRECTOR, INFORMATION SECURITY OVERSIGHT OFFICE

Mr. WILSHUSEN. Thank you, Mr. Chairman and members of the committee. I am pleased to be here today to discuss our prelimi-

nary observations on the Department of Defense's process for determining the eligibility of industry personnel for security clearances.

Individuals working for industry are taking on a significant role in national security work for DOD and other Federal agencies. Because many of these jobs require access to classified information, industry personnel need security clearances. As of September 30, 2003, industry workers held about one-third of the approximately 2 million DOD-issued clearances.

The timeliness of the Department's personnel security clearance process has historically been at issue. Our reviews, as well as those of others, including this committee, have identified backlogs and delays in determining clearance eligibility for service members, Federal employees, and industry personnel. In response to your request, we reviewed DOD's process for determining clearance eligibility for industry personnel, and a report with our recommendations is forthcoming.

Mr. Chairman, based on our preliminary observations, my main message today is that DOD continues to experience sizable backlogs and delays in processing clearance requests for industry personnel, and that these delays can have adverse effects for national security and contractors performing classified work.

As of March 31, 2004, the backlog for industry personnel was estimated to be roughly 188,000 cases. To provide perspective on the size of the backlog, DOD made about 100,000 eligibility determinations for industry personnel in fiscal year 2003. DOD is also taking longer to determine clearance eligibility. From fiscal year 2001 through 2003, the average time increased by 56 days to over 1 year, significantly exceeding the timeframes established for making these determinations.

Delays in completing reinvestigations of industry personnel and others who are doing classified work can increase national security risks because the longer individuals hold clearances, the more likely they are to be working with critical information and systems. In addition, delays in determining clearance eligibility can affect the timeliness, quality, and cost of contractor performance on defense contracts.

Several factors impede DOD's ability to eliminate the backlogs and delays. These include the large number of clearance requests, an increase in the proportion of requests for top secret clearances, inaccurate workload projections, and an imbalance between the investigative and adjudicative work forces and their workloads.

In addition, industry contractors cited under-utilization of reciprocity as an obstacle to timely eligibility determinations. Although reciprocity of clearances appears to be working throughout most of DOD, reciprocity of access to certain information and programs within DOD and by certain agencies is sometimes problematic for industry personnel.

DOD is considering several initiatives that might reduce the backlogs and processing times. For examples, DOD is considering conducting phased reinvestigations, establishing a single adjudicative facility for industry, and reevaluating investigative standards and adjudicative guidelines.

Although DOD has several plans to address elements of the backlog problem, it does not have an integrated, comprehensive

management plan for eliminating the backlog, reducing delays, and overcoming the impediments that allow such problems to recur. Without such a comprehensive plan, DOD's success in eliminating the backlog may be limited.

Mr. Chairman, this concludes my opening statement and I will be happy to answer any questions you or other members of the committee may have.

[The prepared statement and accompanying report of Mr. Wilshusen follow:]

United States General Accounting Office

GAO

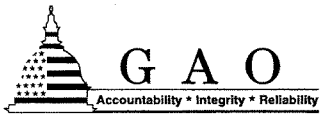
Testimony
Before the Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EDT
Thursday, May 6, 2004

DOD PERSONNEL CLEARANCES

Preliminary Observations Related to Backlogs and Delays in Determining Security Clearance Eligibility for Industry Personnel

Statement of Gregory C. Wilshusen, Acting Director
Defense Capabilities and Management



GAO-04-202T

GAO
Accountability · Integrity · Reliability

Highlights

Highlights of GAO-04-202T, a testimony before the House Committee on Government Reform

Why GAO Did This Study

Because of increased awareness of threats to national security and efforts to privatize federal jobs, the demand for security clearances for government and industry personnel has increased. Industry personnel are taking on a greater role in national security work for the Department of Defense (DOD) and other federal agencies. Because many of these jobs require access to classified information, industry personnel need security clearances. As of September 30, 2003, industry workers held about one-third of the approximately 2 million DOD-issued security clearances.

Terrorist attacks have heightened national security concerns and underscored the need for a timely, high-quality personnel security clearance process. However, GAO's past work found that DOD had a clearance backlog and other problems with its process. GAO was asked to review the clearance eligibility determination process and backlog for industry personnel.

This testimony presents our preliminary observations on the security clearance process for industry personnel and describes (1) the size of the backlog and changes in the time needed to issue eligibility determinations, (2) the impediments to reducing the backlog and delays, and (3) some of the initiatives that DOD is considering to eliminate the backlog and decrease the delays. Later this month, we plan to issue our final report.

www.gao.gov/cgi-bin/getrpt?GAO-04-202T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

May 6, 2004

DOD PERSONNEL CLEARANCES

Preliminary Observations Related to Backlogs and Delays in Determining Security Clearance Eligibility for Industry Personnel

What GAO Found

On the basis of our preliminary observations, long-standing backlogs and delays in determining security clearance eligibility for industry personnel continue to exist and can have adverse effects. DOD's security clearance backlog for industry personnel was roughly 188,000 cases as of March 31, 2004. The backlog included estimates by the Defense Security Service (DSS)—the agency responsible for administering DOD's personnel security investigations program—that consisted of

- more than 61,000 reinvestigations (required for renewing clearances) that were overdue but had not been submitted to DSS,
- over 101,000 new DSS investigations or reinvestigations that had not been completed within DOD's established time frames, and
- over 25,000 cases awaiting adjudication (a determination of clearance eligibility) that had not been completed within DOD's established time frames.

From fiscal year 2001 through fiscal year 2003, the average time that it took DOD to determine clearance eligibility for industry personnel increased by 56 days to over 1 year. Delays in completing reinvestigations of industry personnel and others doing classified work can increase national security risks. In addition, delays in determining clearance eligibility can affect the timeliness, quality, and cost of contractor performance on defense contracts.

Several impediments hinder DOD's ability to eliminate the backlog and decrease the amount of time needed to determine clearance eligibility for industry personnel. Impediments include a large number of new clearance requests; an increase in the proportion of requests for top secret clearances, which require more time to process; inaccurate workload projections for both the number and type of clearances needed for industry personnel; and the imbalance between workforces and workloads. Industrial contractors cited the lack of full reciprocity (the acceptance of a clearance and access granted by another department, agency, or military service) as an obstacle that can cause industry delays in filling positions and starting work on government contracts. Furthermore, DOD does not have an integrated, comprehensive management plan for addressing the backlog and delays.

DOD is considering a number of initiatives to supplement actions that it has implemented in recent years to reduce the backlogs and the time needed to determine eligibility for a security clearance. Additional initiatives include (1) conducting a phased, periodic reinvestigation; (2) establishing a single adjudicative facility for industry; and (3) reevaluating investigative standards and adjudicative guidelines. GAO's forthcoming report will provide a more complete discussion of these and other initiatives.

Mr. Chairman and Members of the Committee:

I am pleased to be here today to discuss our preliminary observations on the process the Department of Defense (DOD) uses to determine security clearance eligibility for industry personnel.

For a variety of reasons, including an increased awareness of threats to our national security resulting from the terrorist attacks on the United States on September 11, 2001, and efforts over the past decade to privatize federal jobs, the demand for security clearances for both government employees and industry personnel has increased over the last few years. Individuals working for industry are playing an increasingly larger role in national security work conducted by DOD and other federal agencies. Many industry personnel hold jobs that allow them to work on classified programs and activities and that require access to classified information. To handle classified information, industry personnel must hold a security clearance. As of September 30, 2003, industry personnel held about 682,000 (or about 34 percent) of the approximately 2 million DOD-issued security clearances.

Terrorist attacks have heightened national security concerns and have highlighted the need for a timely, high-quality personnel security clearance process. As part of a three-stage process, DOD determines whether industry personnel are eligible for a security clearance by conducting a background investigation and adjudication (determining eligibility for access to classified information). However, some government and industry officials have recently expressed concern about the security clearance backlog—overdue security clearance reinvestigations[1] that have not been requested and new investigations and adjudications that have not been completed within established time frames—and the amount of time it takes to determine eligibility for a security clearance for industry personnel.

Since at least the late 1990s, the timeliness of DOD's personnel security clearance process has been at issue. As our previous work has shown, backlogs and delays in personnel security investigations and adjudications historically have been problems for DOD, and they affect industry

[1] Reinvestigations are conducted periodically to determine whether an individual's security clearance should be renewed.

personnel as well as service members and civilian employees.[2] In February and September 2000 testimonies before the Subcommittee on National Security, Veterans Affairs, and International Relations, House Committee on Government Reform,[3] we noted our concerns about the amount of time needed to obtain clearances and that DOD had historically reported a large backlog of overdue but not submitted reinvestigations for security clearances. In our February 2004 report, for example, we identified several impediments that hinder DOD's ability to eliminate its security clearance backlog and made recommendations for decreasing the backlog and improving timeliness.[4] Likewise, this committee reported that DOD's personnel security investigations backlog poses a threat to national security and recommended actions to address the backlog.[5]

Mr. Chairman, in June 2003, you and the Vice Chairman of this committee asked us to review the process DOD uses to determine security clearance eligibility for industry personnel. Later this month, we plan to provide you with a report containing the final results and our recommendations.

Today, I will present our preliminary observations on DOD's security clearance process for industry personnel. Specifically, I will discuss (1) the size of the backlog and changes during the last 3 fiscal years in the time needed to issue eligibility determinations, (2) the impediments to reducing the backlog and delays, and (3) some of the initiatives that DOD is considering to eliminate the backlog and decrease the delays.

[2] See U.S. General Accounting Office, *DOD Personnel: More Consistency Needed in Determining Eligibility for Top Secret Clearances*, GAO-01-465 (Washington, D.C.: Apr. 18, 2001); U.S. General Accounting Office, *DOD Personnel: More Actions Needed to Address Backlog of Security Clearance Reinvestigations*, GAO/NSIAD-00-215 (Washington, D.C.: Aug. 24, 2000); and U.S. General Accounting Office, *DOD Personnel: Inadequate Personnel Security Investigations Pose National Security Risks*, GAO/NSIAD-00-12 (Washington, D.C.: Oct. 27, 1999).

[3] See U.S. General Accounting Office, *DOD Personnel: Inadequate Personnel Security Investigations Pose National Security Risks*, GAO/T-NSIAD-00-65 (Washington, D.C.: Feb. 16, 2000) and U.S. General Accounting Office, *DOD Personnel: More Accurate Estimate of Overdue Security Clearance Reinvestigations Is Needed*, GAO/T-NSIAD-00-246 (Washington, D.C.: Sept. 20, 2000).

[4] See U.S. General Accounting Office, *DOD Personnel Clearances: DOD Needs to Overcome Impediments to Eliminating Backlog and Determining Its Size*, GAO-04-344 (Washington, D.C.: Feb. 9, 2004).

[5] See Committee on Government Reform, *Defense Security Service: The Personnel Security Investigations [PSI] Backlog Poses a Threat to National Security*, H.R. 107-767 (Oct. 24, 2002).

In conducting this review, we examined DOD policy guidance, regulations, instructions, and statistical evidence on the security clearance process for industry personnel. In addition, we reviewed reports by GAO, DOD, congressional staff, and other government entities. We also interviewed DOD and industry officials, observed the procedures used to process clearance information, and assessed the reliability of databases. We determined that the data for fiscal years 2001 and thereafter were sufficiently reliable for the purpose of our work. At the end of my statement is a list of related GAO products. We conducted our review from July 2003 through April 2004 in accordance with generally accepted government auditing standards.

Summary

Long-standing backlogs and delays in determining security clearance eligibility for industry personnel continue to exist and can have adverse effects. As of March 31, 2004, DOD estimated that its security clearance backlog for industry personnel was roughly 188,000 cases. DOD identified more than 61,000 reinvestigations that were overdue but had not been submitted, over 101,000 backlogged investigations, and over 25,000 backlogged adjudications. In the 3-year period from fiscal year 2001 through fiscal year 2003, the average time that it took DOD to determine clearance eligibility for industry personnel increased by 56 days to over 1 year. Delays in initiating reinvestigations for individuals working on classified programs and activities can increase national security risks while delays in determining eligibility for clearances for industry personnel can affect the timeliness, quality, and cost of contractor performance on defense contracts. Such delays prevent industry personnel from beginning or continuing work on classified programs and activities, hinder industrial contractors from hiring the most experienced and best qualified personnel, increase the time needed to complete national-security-related contracts, and increase costs to the federal government.

A number of impediments hinder DOD's ability to eliminate the backlog and decrease the amount of time needed to determine eligibility for security clearances for industry personnel. Impediments include large investigative and adjudicative workloads resulting from a large number of clearance requests in recent years; an increase in the proportion of requests requiring top secret clearances, which take longer and are more expensive to complete than secret clearances; inaccurate workload projections; and the imbalance between workforces and workloads. Industrial contractors cited the lack of full reciprocity—a policy that requires acceptance by an agency of an equivalent personnel security

clearance and access granted by another agency—as an impediment that can cause industry contractors delays in filling positions and starting work on government contracts. Furthermore, DOD does not have a management plan to address the impediments in a comprehensive and integrated manner.

DOD is considering a number of initiatives to reduce the backlog and the amount of time needed to determine eligibility for a security clearance. Among those steps that DOD is exploring are conducting a phased periodic reinvestigation; establishing a single adjudicative facility for industry; and reevaluating investigative standards and adjudicative guidelines. Even if these initiatives prove promising, they face obstacles—such as the need to change investigative standards, coordinate these policy changes with other agencies, and ensure reciprocity—that could prevent their implementation or limit their use. Our May 2004 evaluative report will provide a more complete discussion of these and other initiatives.

Background

In March 1997, a White House memorandum implemented adjudicative guidelines, temporary eligibility standards, and investigative standards governmentwide.[6] The National Security Council is responsible for overseeing these guidelines and standards. Within DOD, the Office of the Under Secretary of Defense for Intelligence (OUSD (I)) is responsible for coordinating and implementing DOD-wide policies related to access to classified information.[7] Within OUSD (I), the Defense Security Service (DSS) is responsible for conducting background investigations and administering the personnel security investigations program for DOD and 24 other federal agencies that allow industry personnel access to classified

[6] See The White House, "Implementation of Executive Order 12968," Memorandum (Washington, D.C.: Mar. 24, 1997). This memorandum includes the *Investigative Standards for Background Investigations for Access to Classified Information* and *Adjudicative Guidelines for Determining Eligibility for Access to Classified Information*. It approves the adjudicative guidelines, temporary eligibility standards, and investigative standards required by Executive Order No. 12968, *Access to Classified Information* (Aug. 4, 1995).

[7] Previously, this responsibility resided within the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence. OUSD (I) was created in 2002 by the Bob Stump National Defense Authorization Act for Fiscal Year 2003, Pub. L. No. 107-314 § 901 (Dec. 2, 2002).

information.[8] DSS's Defense Industrial Security Clearance Office (DISCO) adjudicates cases that contain only favorable information or minor security issues. The Defense Office of Hearings and Appeals (DOHA) within DOD's Office of General Counsel adjudicates cases that contain more serious security issues.

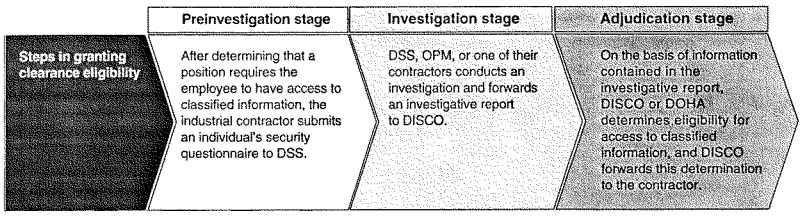
As with military members and federal workers, industry personnel must obtain a security clearance to gain access to classified information, which is categorized into three levels: top secret, secret, and confidential. Individuals who need access to classified information over a long period are required to periodically renew their clearance (a reinvestigation). The time frames for reinvestigations are 5 years for top secret clearances, 10 years for secret clearances, and 15 years for confidential clearances.[9]

To ensure the trustworthiness, judgment, and reliability of contractor personnel in positions requiring access to classified information, DOD relies on a three-stage personnel security clearance process that includes (1) determining that the position requires a clearance and, if so, submitting a request for a clearance to DSS, (2) conducting an initial investigation or reinvestigation, and (3) using the investigative report to determine eligibility for access to classified information—a procedure known as "adjudication." Figure 1 depicts this three-stage process and the federal government offices that have the lead responsibility for each stage.

[8] Executive Order No. 10865, *Safeguarding Classified Information within Industry* (Feb. 20, 1960), which was amended by Executive Order No. 12829, *National Industrial Security Program* (Jan. 6, 1993), authorizes DOD to reach agreement with other federal departments and agencies to extend its regulations concerning authorizations for access to classified information by industry. Three federal agencies (the Department of Energy, the Central Intelligence Agency, and Nuclear Regulatory Commission) also may grant security clearances to industry personnel who work on national-security-related programs.

[9] See *Adjudicative Guidelines for Determining Eligibility for Access to Classified Information*, 32 C.F.R. Part 147, Subpart B, Attach. A and Attach. C (2003).

Figure 1: DOD's Personnel Security Clearance Process for Industry Personnel



Sources: DSS and DOHA.

Note: Cases involving access to sensitive compartmented information (see footnote 21) are sent through the requesting agency's central adjudication facility for adjudication.

In the preinvestigation stage, the industrial contractor must determine that a position requires the employee to have access to classified information. If a clearance is needed, the industry employee completes a personnel security questionnaire, and the industrial contractor submits it to DSS. All industry requests for a DOD-issued clearance are submitted to DSS while requests for military members and federal employees are submitted to either DSS or the Office of Personnel Management (OPM).

In the investigation stage, DSS, OPM, or one of their contractors conducts the actual investigation of the industry employee by using standards established governmentwide in 1997 and implemented by DOD in 1998.[10] As table 1 shows, the type of information gathered in an investigation depends on the level of clearance needed and whether an initial investigation or a reinvestigation is required. DSS forwards the completed investigative report to DISCO.

[10] See Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, "Personnel Security Investigations and Adjudications," Memorandum (Washington, D.C.: Nov. 10, 1998). In implementing the federal adjudicative guidelines, DOD Directive 5200.2, *DOD Personnel Security Program* (Apr. 9, 1999), sets forth the policies and procedures for granting DOD military, civilian, and industry personnel access to classified information. The policies and procedures for granting industrial 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).

Table 1: Information Gathered to Determine Eligibility for a Security Clearance

	Type of security clearance		
	Confidential or secret	Top secret	
Type of information gathered	Initial investigation or reinvestigation	Initial investigation	Reinvestigation
1. Personnel security questionnaire: The subject's self-reported answers on a paper SF-86 form or an electronic form	X	X	X
2. National agency check: Data from Federal Bureau of Investigation, military records centers, Treasury, etc.	X	X	X
3. Credit check: Data from credit bureaus where the subject lived/worked/attended school for at least 6 months	X	X	X
4. Local agency checks: Data from law enforcement agencies where the subject lived/worked/attended school during past 5 years	X	X	X
5. Date and place of birth: Corroboration of information supplied on the personnel security questionnaire	X	X	
6. Citizenship: For individuals born outside of the United States, verification of U.S. citizenship directly from the appropriate registration authority		X	
7. Education: Corroboration of most recent or significant claimed attendance, degree, or diploma		X	X
8. Employment: Review of employment records and interviews with workplace references, such as supervisors and coworkers		X	X
9. References: Data from interviews with subject-identified and investigator-developed leads		X	X
10. National agency check for spouse or cohabitant: National agency check without fingerprint		X	X
11. Former spouse: Data from interview(s) conducted with spouse(s) divorced within the last 10 years		X	X
12. Neighborhoods: Interviews with neighbors and verification of residence through records check		X	X
13. Public records: Verification of issues, such as bankruptcy, divorce, and criminal and civil court cases		X	X
14. Subject interview: To collect relevant data, resolve significant inconsistencies, or both		X	X

Source: OSS.

In the adjudicative stage, DISCO uses the information from the investigative report to determine whether an individual is eligible for a security clearance. If the report is determined to be a "clean" case—a case that contains no potential security issue or minor issues—then DISCO adjudicators determine eligibility for a clearance. However, if the case is an "issue" case—a case containing issues that might disqualify an individual for a clearance (e.g., foreign connections or drug- or alcohol-related problems)—then the case is forwarded to DOHA adjudicators for the clearance-eligibility decision. Regardless of which office determines eligibility, DISCO issues the clearance-eligibility decision and forwards this determination to the industrial contractor. All adjudications are based on 13 federal adjudicative guidelines established governmentwide in 1997 and implemented by DOD in 1998.

Recent legislation could affect DOD's security clearance process. The National Defense Authorization Act for Fiscal Year 2004 authorized the transfer of DOD's personnel security investigative functions and more than 1,800 investigative employees to OPM.[11] However, as of March 31, 2004, this transfer had not taken place. The transfer can occur only after the Secretary of Defense certifies to Congress that certain conditions can be met and the Director of OPM concurs with the transfer.

Long-standing Backlogs and Delays in Determining Security Clearance Eligibility for Industry Personnel Continue to Exist and Can Have Adverse Effects

DOD's security clearance backlog for industry personnel is sizeable, and the average time needed to determine eligibility for a clearance increased during the last 3 fiscal years to over 1 year. DSS has established case-completion time frames for both its investigations and adjudications. For investigations, the time frames range from 75 to 180 days, depending on the investigative requirements.[12] For DISCO adjudications, the time frames are 3 days for initial clearances and 30 days for periodic reinvestigations. DOHA's time frame is to maintain a steady workload of adjudicating 2,150 cases per month within 30 days of receipt. Cases exceeding these time frames are considered backlogged.

[11] See Pub. L. No. 108-136, § 906 (Nov. 24, 2003).

[12] DSS's performance goal is to complete at least 75 percent of each type of investigation within the specified time limits. However, monitoring of the backlog requires a determination of whether each investigation was completed within the time frame—not whether an aggregate performance goal was met for a particular type of investigation.

- **Sizeable backlog continues to exist**—As of March 31, 2004, the security clearance backlog for industry personnel was roughly 188,000 cases. This estimate is the sum of four separate DSS-supplied estimates: over 61,000 reinvestigations that were overdue but had not been submitted, over 101,000 ongoing DSS investigations, over 19,000 cases awaiting adjudication at DISCO, and more than 6,300 cases awaiting adjudication at DOHA that had exceeded the case-completion time frames established for conducting them. However, as of March 31, 2004, DOHA independently reported that it had eliminated its adjudicative backlog.

Moreover, the size of the total DSS-estimated backlog for industry personnel doubled during the 6-month period ending on March 31, 2004, as the comparison in table 2 shows. This comparison does not include the backlog of overdue reinvestigations that have not been submitted because DSS was not able to estimate that backlog as of September 30, 2003.

Table 2: Comparison of Backlog Sizes As of September 30, 2003, and March 31, 2004

	Estimated number of backlogged cases for industry personnel		Increase in backlog	
Type of backlog	Sept. 30, 2003	Mar. 31, 2004	Number of cases	Percentage of increase
Investigative backlog	44,600	101,000	56,400	126
Adjudicative backlog at DISCO	12,800	19,000	6,200	48
Adjudicative backlog at DOHA	4,500	6,300	1,800	40
Total	**61,900**	**126,300**	**64,400**	**104**

Sources: DSS and the Case Control Management System (data); GAO (analysis).

Note: Although DSS provided the backlog estimates in table 2, DOHA independently reported that, as of March 31, 2004, it had eliminated its adjudicative backlog.

The industry backlogs for investigations and adjudications represent about one-fifth of the DOD-wide backlog for investigations and adjudications as of September 30, 2003 (the date of the most recent DOD-wide data). On that date, the estimated size of the investigative backlog for industry personnel amounted to roughly 44,600 cases, or 17 percent of the larger DOD-wide backlog of approximately 270,000 cases, which included military members, federal employees, and industry personnel. Similarly, the estimated size of the adjudicative backlog for industry personnel totaled roughly 17,300 cases, or 19 percent of the approximately 93,000 cases in the DOD-wide adjudicative backlog on that date.

Furthermore, the size of the industrial personnel backlog may be underestimated. In anticipation of the authorized transfer of the

investigative function from DSS to OPM, DSS had opened relatively few cases between October 1, 2003, and March 31, 2004. More specifically, DSS had not opened almost 69,200 new industry personnel requests received in the first half of fiscal year 2004. Because these requests have not been opened and investigations begun, they are not part of the 188,000 case backlog identified above. An unknown number of these cases might have already exceeded the set time frames for completing the investigation.

- **Average time to determine clearance eligibility has increased**—In the 3-year period from fiscal year 2001 through fiscal year 2003, the average time that DOD took to determine clearance eligibility for industry personnel increased from 319 days to 375 days, an increase of 18 percent. (See table 3.) During fiscal year 2003, DOD took an average of more than 1 year from the time DSS received a personnel security questionnaire to the time it issued an eligibility determination. From fiscal year 2001 through fiscal year 2003, the number of days to determine clearance eligibility for clean cases increased from 301 days to 332 days, whereas the time increased for issue cases from 516 days to 615 days.

Table 3: Average Number of Days Needed to Determine Eligibility for a Security Clearance for Industry Personnel, Fiscal Years 2001-3

	Average number of days to determine eligibility for a security clearance for industry personnel		
Fiscal year	All industry cases	Clean cases[a]	Issue cases[b]
2003	375	332	615
2002	343	316	629
2001	319	301	516

Sources: DISCO and the Case Control Management System.

Note: Although DSS's case management system can provide the total elapsed time between opening a case and issuing the final security clearance eligibility determination, it is not capable of generating separate time estimates for the intermediate stages of the clearance process. Nor does it have the capability to identify how much time DOHA needed to adjudicate issue cases. Therefore, all of the time-based findings include the time period beginning when personnel security questionnaires were entered into the case management system and ending when DISCO notified the industrial contractor of the DISCO or DOHA adjudicators' decisions to grant a clearance.

[a]Includes investigative time and DISCO review time.

[b]Includes investigative time, DISCO and DOHA review time, and additional time when some cases were sent back for additional investigation or were appealed after a denial or revocation of a clearance.

- **Backlogs and delays can have adverse effects**—Delays in renewing security clearances for industry personnel and others who are doing classified work can lead to a heightened risk of national security breaches.

In a 1999 report, the Joint Security Commission II pointed out that delays in initiating reinvestigations create risks to national security because the longer the individuals hold clearances, the more likely they are to be working with critical information and systems.[13] In addition, delays in determining security clearance eligibility for industry personnel can affect the timeliness, quality, and cost of contractor performance on defense contracts. According to a 2003 Information Security Oversight Office[14] report, industrial contractor officials who were interviewed said that delays in obtaining clearances cost industry millions of dollars per year and affect personnel resources.[15] The report also stated that delays in the clearance process hampered industrial contractors' ability to perform duties required by their contracts and increased the amount of time needed to complete national-security-related contracts. Industrial contractors told us about cases in which their company hired competent applicants who already had the necessary security clearances, rather than individuals who were more experienced or qualified but did not have a clearance. Industry association representatives told us that defense contractors might offer monetary incentives to attract new employees with clearances—for example, a $15,000 to $20,000 signing bonus for individuals with a valid security clearance, and a $10,000 bonus to current employees who recruit a new employee with a clearance. In addition, defense contractors may hire new employees and begin paying them, but not be able to assign any work to them—sometimes for a year or more—until they obtain a clearance. Contractors may also incur lost-opportunity costs if prospective employees decide to work elsewhere rather than wait to get a clearance.

[13] See Joint Security Commission II, *Report by the Joint Security Commission II* (Aug. 24, 1999), pp. 5-6.

[14] Executive Order No. 12829, *National Industrial Security Program*, Jan. 6, 1993, requires the Director of the Information Security Oversight Office to implement and monitor the National Industrial Security Program and oversee agency, contractor, licensee, and grantee actions; review all agency implementing regulations, internal rules or guidelines; and gives the Director the authority to conduct periodic on-site reviews of the implementation of the program by each program member that has access to classified information or stores it. This office is part of the National Archives and Records Administration.

[15] See Information Security Oversight Office, *The National Industrial Security Program, Industry's Perspective: Making Progress, but Falling Short of Potential* (2003).

Impediments Hinder Elimination of the Backlog and Reduction of Time Needed to Determine Eligibility for a Clearance

A number of impediments hinder DOD's efforts to eliminate the clearance backlog for industry personnel and reduce the time needed to determine eligibility for a clearance. Impediments include large investigative and adjudicative workloads resulting from a large number of clearance requests in recent years and an increase in the proportion of requests requiring top secret clearances, inaccurate workload projections, and the imbalance between workforces and workloads. The underutilization of reciprocity is an impediment that industrial contractors cited as an obstacle to timely eligibility determinations. Furthermore, DOD does not have a management plan that could help it address many of these impediments in a comprehensive and integrative manner.

- **Large number of clearance requests**—The large number of clearance requests that DOD receives annually for industry personnel, military members, and federal employees taxes a process that already is experiencing backlogs and delays. In fiscal year 2003, DOD submitted over 775,000 requests for investigations to DSS and OPM, about one-fifth of which (almost 143,000 requests) were for industry personnel. Table 4 shows an increase in the number of DOD eligibility determinations for industry personnel made during each of the last 3 years.[16] DOD issued about 63,000 more eligibility determinations for industry personnel in fiscal year 2003 than it did 2 years earlier, an increase of 174 percent. During the same period, the average number of days required to issue an eligibility determination for industry personnel grew by 56 days, or about 18 percent. In other words, the increase in the average wait time was small compared to the increase in the number of cases.

Table 4: Number of Clearance-Eligibility Determinations for Industry Personnel, Fiscal Years 2001-3

	Number of clearance-eligibility determinations for industry personnel		
Fiscal year	All industry cases	Clean cases	Issue cases
2003	99,652	87,172	12,480
2002	86,226	78,836	7,390
2001	36,370	33,294	3,076

Source: DISCO and the Case Control Management System.

[16] The outcomes of the clearance requests are eligibility determinations, but the determinations may be made in the year subsequent to the year when the request was submitted.

- **Increase in the proportion of requests for top secret clearances**—From fiscal year 1995 through fiscal year 2003, the proportion of all requests requiring top secret clearances for industry personnel grew from 17 to 27 percent. According to OUSD (I), top secret clearances take eight times more investigative effort to complete and three times more adjudicative effort to review than do secret clearances. The increased demand for top secret clearances also has budget implications for DOD. In fiscal year 2003, security investigations obtained through DSS cost $2,640 for an initial investigation for a top secret clearance, $1,591 for a reinvestigation of a top secret clearance, and $328 for an initial investigation for a secret clearance. Thus, over a 10-year period, DOD would spend $4,231 (in current-year dollars) to investigate and reinvestigate an industry employee for a top secret clearance, a cost 13 times higher than the $328 it would require to investigate an individual for a secret clearance.

- **Inaccurate workload projections**—Although DSS has made efforts to improve its projections of industry personnel security clearance requirements, problems remain. For example, inaccurate forecasts for both the number and type of security clearances needed for industry personnel make it difficult for DOD to plan ahead to size its investigative and adjudicative workforce to handle the workload and fund its security clearance program. For fiscal year 2003, DSS reported that the actual cost of industry personnel investigations was almost 25 percent higher than had been projected. DOD officials believed that these projections were inaccurate primarily because DSS received a larger proportion of requests for initial top secret investigations and reinvestigations. Further inaccuracies in projections may result when DOD fully implements a new automated adjudication tracking system, which will identify overdue reinvestigations that have not been submitted DOD-wide.

- **Imbalance between workforces and workloads**—Insufficient investigative and adjudicative workforces, given the current and projected workloads, are additional barriers to eliminating the backlog and reducing security clearance processing times for industry personnel. DOD partially concurred with our February 2004 recommendation to identify and implement steps to match the sizes of the investigative and adjudicative workforces to the clearance request workload. According to an OPM official, DOD and OPM together need roughly 8,000 full-time-equivalent investigative staff to eliminate the security clearance backlogs and deliver

timely investigations to their customers.[17] In our February 2004 report, we estimated that DOD and OPM have around 4,200 full-time-equivalent investigative staff who are either federal employees or contract investigators.[18]

In December 2003, advisors to the OPM Director expressed concerns about financial risks associated with the transfer of DSS's investigative functions and 1,855 investigative staff authorized in the National Defense Authorization Act for Fiscal Year 2004. The advisors therefore recommended that the transfer not occur, at least during fiscal year 2004. On February 6, 2004, DSS and OPM signed an interagency agreement that leaves the investigative functions and DSS personnel in DOD and provides DSS personnel with training on OPM's case management system and investigative procedures as well as access to that system. According to our calculations, if all 1,855 DSS investigative employees complete the 1-week training program as planned, the loss in productively will be equivalent to 35 person-years of investigator time. Also, other short-term decreases in productivity will result while DSS's investigative employees become accustomed to using OPM's system and procedures.

Likewise, an adjudicative backlog of industry personnel cases developed because DISCO and DOHA did not have an adequate number of adjudicative personnel on hand. DISCO and DOHA have, however, taken steps to augment their adjudicative staff. DISCO was recently given the authority to hire 30 adjudicators to supplement its staff of 62 nonsupervisory adjudicators. Similarly, DOHA has supplemented its 23 permanent adjudicators with 46 temporary adjudicators and, more recently, has requested that it be able to hire an appropriate number of additional permanent adjudicators.

- **Reciprocity of access underutilized**—While the reciprocity of security clearances within DOD has not been a problem for industry personnel, reciprocity of access to certain types of information and programs within the federal government has not been fully utilized, thereby preventing some industry personnel from working and increasing the workload on

[17] OPM has estimated that DOD and OPM account for 80 percent of the investigations conducted for the federal government.

[18] See GAO-04-344.

already overburdened investigative and adjudicative staff.[19] According to DOD and industry officials, a 2003 Information Security Oversight Office report on the National Industrial Security Program,[20] and our analysis, reciprocity of clearances appears to be working throughout most of DOD. However, the same cannot be said for access to sensitive compartmented information and special access programs[21] within DOD or transferring clearances and access from DOD to some other agencies. Similarly, a recent report by the Defense Personnel Security Research Center concluded that aspects of reciprocity for industrial contractors appear not to work well and that the lack of reciprocity between special access programs was a particular problem for industry personnel, who often work on many of these programs simultaneously.[22]

Industry association officials told us that reciprocity of access to certain types of information and programs, especially the lack of full reciprocity in the intelligence community, is becoming more common and one of the top concerns of their members. One association provided us with several examples of access problems that industry personnel with DOD-issued security clearances face when working with intelligence agencies. For example, the association cited different processes and standards used by intelligence agencies, such as guidelines for (1) the type of investigations and required time frames, (2) the type of polygraph tests, and (3) not accepting adjudication decisions made by other agencies.

[19] Reciprocity, which is required by Executive Order No. 12968, is a policy that requires background investigations and eligibility determinations conducted under the order be mutually and reciprocally accepted by all agencies, except when an agency has substantial information indicating that an employee may not satisfy the standards under this order. Reciprocity also involves the ability to transfer (1) an individual's existing, valid security clearance and (2) access from one department, agency, or military service to another or from the federal government to the private sector (and vice versa) when the individual changes jobs without having to grant another clearance or access.

[20] See Information Security Oversight Office, *The National Industrial Security Program, Industry's Perspective: Making Progress, but Falling Short of Potential* (2003).

[21] Sensitive compartmented information is classified intelligence information derived from intelligence sources, methods, or analytical processes, which is handled by systems established by the Director of Central Intelligence. A special access program is a sensitive program that imposes need-to-know and access controls beyond those normally provided for access to confidential, secret, or top secret information.

[22] See Defense Personnel Security Research Center, *Reciprocity: A Progress Report*, PERSEREC Technical Report 04-2 (Monterey, Calif.: Apr. 1, 2004).

In addition to the reciprocity concerns relating to access to sensitive compartmented information and special access programs, industry officials identified additional reciprocity concerns. First, DSS and contractor association officials told us that some personnel with an interim clearance could not start work because an interim clearance does not provide access to specific types of national security information, such as sensitive compartmented information, special access programs, North Atlantic Treaty Organization data, and restricted data. [23] Second, intelligence agencies do not always accept clearance reinstatements and conversions (e.g., a security clearance may be reactivated depending on the recency of the investigation and the length of time since the clearance was terminated). Third, the Smith Amendment—with exceptions—prohibits an individual with a clearance from being eligible for a subsequent DOD clearance if certain prohibitions (e.g., unlawful user of a controlled substance) are applicable.[24]

- **Lack of overall management plan**—Finally, DOD has numerous plans to address pieces of the backlog problem but does not have an overall management plan to eliminate permanently the current investigative and adjudicative backlogs, reduce the delays in determining clearance eligibility for industry personnel, and overcome the impediments that could allow such problems to recur. These plans do not address process wide objectives and outcome-related goals with performance measures, milestones, priorities, budgets, personnel resources, costs, and potential obstacles and options for overcoming the obstacles.

[23] Under the Atomic Energy Act of 1954 (as amended), the term "restricted data" means all data (information) concerning the (1) design, manufacture, or utilization of atomic weapons, (2) the production of special nuclear material, or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the restricted data category pursuant to § 142 of the Act. Pub. L. No. 83-703 § 11 (Aug. 30, 1954), codified at 42 U.S.C. § 2014.

[24] See Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001, Pub. L. No. 106-398, § 1071 (Oct. 30, 2000) (codified at 10 U.S.C. § 986).

DOD Is Considering Several Initiatives to Decrease the Backlog and Time Period Needed to Obtain Eligibility for a Clearance

DOD and industry association officials have suggested several initiatives to reduce the backlog and delays in issuing eligibility for a security clearance. They indicated that these steps could supplement actions that DOD has implemented in recent years or has agreed to implement as a result of our recommendations or those of others. Even if positive effects would result from these initiatives, other obstacles, such as the need to change investigative standards, coordinate these policy changes with other agencies, and ensure reciprocity, could prevent their implementation or limit their use. Today, I will discuss three of the suggested initiatives. Our final report to you will provide a more complete evaluation of these and other initiatives.

- **Conducting a phased periodic reinvestigation**—A phased approach to periodic reinvestigations for top secret clearances involves conducting a reinvestigation in two phases; the second phase would be conducted only if potential security issues were identified in the initial phase. Phase 1 information is obtained through a review of the personnel security questionnaire, subject and former spouse interviews, credit checks, a national agency check on the subject and former spouse or current cohabitant, local agency checks, records checks, and interviews with workplace personnel. If one or more issues are found in phase 1, then phase 2 would include all of the other types of information gathered in the current periodic reinvestigation for a top secret investigation. Recent research has shown that periodic reinvestigations for top secret clearances conducted in two phases can save at least 20 percent of the normal effort with almost no loss in identifying critical issues for adjudication.[25] According to DSS, this initiative is designed to use the limited investigative resources in the most productive manner and reduce clearance-processing time by eliminating the routine use of low-yield information sources on many investigations and concentrating information-gathering efforts on high-yield sources. While analyses have not been conducted to evaluate how the implementation of phasing would affect the investigative backlog, the implementation of phasing could be a factor in reducing the backlog by decreasing some of the hours of fieldwork required in some reinvestigations. Even if additional testing confirms promising earlier findings that the procedure very rarely fails to identify critical issues, several obstacles, such as noncompliance with existing governmentwide investigative standards and reciprocity

[25] See Defense Personnel Security Research Center, *A New Approach to the SSBI-PR: Assessment of a Phased Reinvestigation*, PERSEREC Technical Report 01-6 (Monterey, Calif.: Oct. 29, 2001) and *Implementation of the Phased SSBI-PR at DSS: An Evaluation with Recommendations*, PERSEREC Technical Report 04-X (Monterey, Calif.: in press).

problems, could prevent the implementation or limit the use of this initiative.

- **Establishing a single adjudicative facility for industry**—Under this initiative, DOD would consolidate DOHA's adjudicative function with that of DISCO's to create a single adjudicative facility for all industry personnel cases. At the same time, DOHA would retain its hearings and appeals function. According to OUSD (I) officials, this consolidation would streamline the adjudicative process for industry personnel and make it more coherent and uniform. A single adjudicative facility would serve as the clearinghouse for all industrial contractor-related issues. As part of a larger review of DOD's security clearance processes, DOD's Senior Executive Council is considering this consolidation. An OUSD (I) official told us that the consolidation would provide greater flexibility in using adjudicators to meet changes in the workload and could eliminate some of the time required to transfer cases from DISCO and to DOHA. If the consolidation occurred, DISCO officials said that their operations would not change much, except for adding adjudicators. On the other hand, DOHA officials said that the current division between DISCO and DOHA of adjudicating clean versus issue cases works very well and that combining the adjudicative function for industry into one facility could negatively affect DOHA's ability to prepare denials and revocations of industry personnel clearances during appeals. They told us that the consolidation would have very little impact on the timeliness and quality of adjudications.

- **Evaluation of the investigative standards and adjudicative guidelines**—This initiative would involve an evaluation of the investigative standards used by personnel security clearance investigators to help identify requirements that do not provide significant information relevant for adjudicative decisions. By eliminating the need to perform certain tasks associated with these requirements, investigative resources could be used more efficiently. For example, DSS officials told us that less than one-half of one percent of the potential security issues identified during an investigation are derived from neighborhood checks; however, this information source accounts for about 14 percent of the investigative time. The modification of existing investigative standards would involve using risk management principles based on a thorough evaluation of the potential loss of information. Like a phased periodic reinvestigation, this initiative would require changes in the governmentwide investigative

standards. In addition, the evaluation and any suggested changes would need to be coordinated within DOD, intelligence agencies, and others.

Mr. Chairman, this concludes my prepared statement. I will be happy to respond to any questions you or other Members of the committee may have at this time.

Appendix I: GAO Contacts and Staff Acknowledgments

GAO Contacts	Gregory C. Wilshusen, (202) 512-6244 Jack E. Edwards, (202) 512-8246
Acknowledgments	Individuals making key contributions to this statement include Mark A. Pross, James F. Reid, William J. Rigazio, and Nancy L. Benco.

Related GAO Products

Industrial Security: DOD Cannot Provide Adequate Assurances That Its Oversight Ensures the Protection of Classified Information. GAO-04-332. Washington, D.C.: March 3, 2004.

DOD Personnel Clearances: DOD Needs to Overcome Impediments to Eliminating Backlog and Determining Its Size. GAO-04-344. Washington, D.C.: February 9, 2004.

DOD Personnel: More Consistency Needed in Determining Eligibility for Top Secret Security Clearances. GAO-01-465. Washington, D.C.: April 18, 2001.

DOD Personnel: More Accurate Estimate of Overdue Security Clearance Reinvestigation Is Needed. GAO/T-NSIAD-00-246. Washington, D.C.: September 20, 2000.

DOD Personnel: More Actions Needed to Address Backlog of Security Clearance Reinvestigations. GAO/NSIAD-00-215. Washington, D.C.: August 24, 2000.

DOD Personnel: Weaknesses in Security Investigation Program Are Being Addressed. GAO/T-NSIAD-00-148. Washington, D.C.: April 6, 2000.

DOD Personnel: Inadequate Personnel Security Investigations Pose National Security Risks. GAO/T-NSIAD-00-65. Washington, D.C.: February 16, 2000.

DOD Personnel: Inadequate Personnel Security Investigations Pose National Security Risks. GAO/NSIAD-00-12. Washington, D.C.: October 27, 1999.

Background Investigations: Program Deficiencies May Lead DEA to Relinquish Its Authority to OPM. GAO/GGD-99-173. Washington, D.C.: September 7, 1999.

Military Recruiting: New Initiatives Could Improve Criminal History Screening. GAO/NSIAD-99-53. Washington, D.C.: February 23, 1999.

Executive Office of the President: Procedures for Acquiring Access to and Safeguarding Intelligence Information. GAO/NSIAD-98-245. Washington, D.C.: September 30, 1998.

Privatization of OPM's Investigations Service. GAO/GGD-96-97R. Washington, D.C.: August 22, 1996.

Cost Analysis: Privatizing OPM Investigations. GAO/GGD-96-121R. Washington, D.C.: July 5, 1996.

Personnel Security: Pass and Security Clearance Data for the Executive Office of the President. GAO/NSIAD-96-20. Washington, D.C.: October 19, 1995.

Privatizing OPM Investigations: Perspectives on OPM's Role in Background Investigations. GAO/T-GGD-95-185. Washington, D.C.: June 14, 1995.

Background Investigations: Impediments to Consolidating Investigations and Adjudicative Functions. GAO/NSIAD-95-101. Washington, D.C.: March 24, 1995.

Security Clearances: Consideration of Sexual Orientation in the Clearance Process. GAO/NSIAD-95-21. Washington, D.C.: March 24, 1995.

Personnel Security Investigations. GAO/NSIAD-94-135R. Washington, D.C.: March 4, 1994.

Nuclear Security: DOE's Progress on Reducing Its Security Clearance Work Load. GAO/RCED-93-183. Washington, D.C.: August 12, 1993.

Personnel Security: Efforts by DOD and DOE to Eliminate Duplicative Background Investigations. GAO/RCED-93-23. Washington, D.C.: May 10, 1993.

DOD Special Access Programs: Administrative Due Process Not Provided When Access Is Denied or Revoked. GAO/NSIAD-93-162. Washington, D.C.: May 5, 1993.

Administrative Due Process: Denials and Revocations of Security Clearances and Access to Special Programs. GAO/T-NSIAD-93-14. Washington, D.C.: May 5, 1993.

Security Clearances: Due Process for Denials and Revocations by Defense, Energy, and State. GAO/NSIAD-92-99. Washington, D.C.: May 6, 1992.

Due Process: Procedures for Unfavorable Suitability and Security Clearance Actions. GAO/NSIAD-90-97FS. Washington, D.C.: April 23, 1990.

GAO's Mission

The General Accounting Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:
Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER

Chairman TOM DAVIS. Thank you very much.

Mr. Benowitz.

Mr. BENOWITZ. Mr. Chairman and members of the committee, I am pleased to testify today on behalf of Office of Personnel Mangement [OPM] Director Kay Coles James on this important topic. Personnel background investigations play an important and unique role in determining whether individuals are suitable for Federal employment, and contribute to an agency's ability to decide whether security clearances can be granted. Taken in this light, the background investigation process is a vital part of our national security efforts, helping ensure that employees and contractors who work for the Federal Government possess the loyalty, experience, training, and skills that our citizens expect and deserve and pose no risk to national security or public trust.

OPM Director James has made the personnel background investigation process a high priority for all Federal agencies, and has taken a leading role in ensuring that OPM staff and each of the agencies understand and take seriously their responsibilities under the Executive order governing security requirements for Government employement. She has worked closely with the heads of all executive branch departments and agencies in this effort to strengthen every link in this program and to aggressively remind her colleagues of the vital need to keep OPM fully informed of the adjudication decisions as prescribed by that Executive order.

OPM conducts background investigations for many Federal agencies on a reimbursable basis. Since the late 1990's, OPM has also performed a substantial number of background investigations for the Department of Defense [DOD]. We receive about 1.1 million investigation requests a year from our client Federal agencies. We witnessed a spike in fiscal year 2002, following the September 11 terrorist attacks on our Nation, when we received nearly 2 million requests. We provide a variety of investigative services, ranging from the basic investigation to determine if individuals are suitable for positions that do not require security clearances, to those for positions which are among the most sensitive in Government. The former are performed largely through our modern and sophisticated computer systems and by mail contacts with State and local police departments, colleges, and universities to confirm education, and former employers to check on experience. For positions requiring a higher level of clearance, we also conduct field investigations that often reach across the country and even to other nations.

Our work flow is always dynamic. New investigation requests are received, as current workload is completed. Our staff members and contract field investigators and support staff team to perform the various tasks associated with the process. Our current pending workload is approximately 340,000 cases, representing a mix of investigation types in various stages of work, ranging from complete case submissions just received from our client agencies to cases where all of the investigative work has been completed and are undergoing the final quality control checks.

Taken together, the total national resources for conducting background investigations for Federal agencies are stretched as a result of the increases we have experienced since fiscal year 2002. Simply put, the demand for background checks currently exceeds our ca-

pacity to provide these services. Under Director James' leadership, we have issued a Request for Proposal [RFP], to increase the number of qualified contractor staff to conduct investigations. National capacity has been an issue the Director has consistently raised, along with strong reservations over the lack of a large base of qualified competition in the investigative industry. We are currently analyzing the proposals and expect to make award decisions fairly soon. Under the requirements of this RFP, the bidders must demonstrate how they will actually increase the number of investigators available. That is, we expect them to recruit and retain new staff to this field, and not simply raid their competitors for employees. The RFP requirement is at least one step toward developing additional trained capacity within the industry. Our estimate is that on a Government-wide basis, we need to increase our field investigation staff by up to 50 percent to meet current and projected demand.

As part of the Defense Authorization Act of 2004, legislation was enacted that would permit Director James, at her discretion, to accept a transfer of function of the DOD investigative staff. She has not yet determined whether she will accept this transfer. However, as part of our efforts to improve the overall coordination of background investigation work in the Federal Government, in February 2004, Director James agreed to provide pending case management and automated processing services for the Department of Defense background investigation program. Under this agreement, Defense Security Service [DSS] staff prioritize their incoming workloads, and forward them to OPM, and they are scheduled on our automated case management system, the Personnel Investigation Processing System [PIPS]. We are training DSS staff at this time to use the system and we expect that training will be completed by June 30, at which time DOD will be able to manage all of their new cases on PIPS.

Mr. Chairman, this concludes my remarks and I would be happy to respond to any questions the committee may have.

[The prepared statement of Mr. Benowitz follows:]

Statement of
Stephen C. Benowitz
Associate Director for Human Resources
Products and Services
Office of Personnel Management

before the

Committee on Government Reform
U.S. House of Representatives

on

Security Clearance Backlogs and
Reciprocity Issues for Defense Industry Personnel

May 6, 2004

Mr. Chairman and Members of the Committee, I am pleased to testify today on behalf of Director Kay Coles James on this important topic. Personnel background investigations play an important and unique role in determining whether individuals are suitable for Federal employment, and contribute to an agency's ability to decide whether security clearances can be granted. Taken in this light, the background investigation process is a vital part of our national security efforts, helping ensure that employees and contractors who work for the Federal Government possess the loyalty, experience, training, and skills that our citizens expect and deserve and pose no risk to national security or public trust.

The Office of Personnel Management (OPM) Director Kay Coles James has made the personnel background investigation process a high priority for all Federal agencies, and has taken a leading role in ensuring that OPM staff and each of the agencies understands and takes seriously their responsibilities under the Executive order, regulations and policies that govern the process. She has worked closely with the heads of all Executive Branch Departments and Agencies in this effort, to strengthen every link in this program and to aggressively remind her colleagues of the vital need to keep OPM fully informed of the adjudication decisions as prescribed by law.

OPM conducts background investigations for many Federal agencies on a reimbursable basis. We are the exclusive source of this work for most of the civilian agencies. Since the late 1990s, OPM has also performed a substantial number of background investigations for the Department of Defense to assist in their efforts to reduce a significant backlog in their reinvestigation program.

OPM receives about 1.1 million investigation requests a year from our client Federal agencies. We witnessed a spike in Fiscal Year 2002, following the September 11 terrorist attacks on our Nation, when we received nearly 2 million requests. OPM provides a variety of investigative services. These range from the basic investigation to determine if individuals are suitable for positions that do not require security clearances, to those for positions which are among the most sensitive in Government. The former are performed largely through our modern and sophisticated computer systems and by mail contacts with State and local police departments, colleges and universities to confirm education, and former employers to check on experience. For positions requiring a higher level of clearance, we also conduct field investigations that often reach across the country and even to other nations.

Our workflow is always dynamic. New investigation requests are received, as current workload is completed. OPM staff members and contract field investigators and support staff team to perform the various tasks associated with the process. Our current pending workload is approximately 340,000 cases, representing a mix of investigation types in various stages of work, ranging from complete case submissions just received from our client agencies to cases where all of the investigative work has been completed and are undergoing the final quality control checks before being returned to the agencies.

Taken together, the total national resources for conducting background investigations for Federal agencies are stretched at the current time, as a result of the increases we have experienced since Fiscal Year 2002. Simply put, the demand for recent background checks currently exceeds capacity of the private sector companies that provide these services. Under Director James' leadership, we have issued a Request for Proposals (RFP) to increase the number of qualified contractor staff to conduct investigations. National capacity has been an issue the Director has consistently raised, along with strong reservations over the lack of a large base of qualified competition in the investigative industry. We are currently analyzing the proposals, and expect to make award decisions fairly soon. Under the requirements of this RFP, the bidders must demonstrate how they will actually increase the number of investigators available. That is, we expect them to recruit and retain new staff to this field, and not simply raid their competitors for employees. This RFP requirement is at least one step toward developing additional trained capacity within the industry. Our estimate is that on a Government-wide basis, we need to increase our field investigation staff by up to 50 percent to meet current and projected demand.

Once OPM completes an investigation, the results are sent to our client agencies. They review the results, and determine if the individual is suitable for Federal employment. If a security clearance is required, the investigation results form part of the basis for determining if a clearance is granted. The suitability review process is called adjudication.

By law, these client agencies are required to complete the adjudication of all background investigations within 90 days of receiving them, and they must report the results back to OPM. This is a critical step in the process of ensuring that the American public can rely on its employees to be well-trained, qualified and suitable for their positions, and can be counted on to support our nation's Constitutional form of government. OPM and its partners offer training for agency personnel security and human resources staff to ensure they have the skills and tools necessary to complete this work. Over the past 6 months, OPM Director James has worked diligently to train agency staff and to push agencies to eliminate the backlog of adjudication decisions flowing back to OPM. In some cases, this required the Director to write to State Governors and Federal agencies to expedite work.

As part of the Defense Authorization Act of 2004, legislation was enacted that would permit the Director of OPM, at her discretion, to accept a transfer of function of the DOD DSS investigative staff. Director James has not yet determined whether she will accept this transfer. However, as part of our efforts to improve the overall coordination of background investigation work in the Federal Government, in February 2004, OPM Director James agreed to provide pending case management and automated processing services for the Department of Defense background investigation program. Under this agreement, Defense Security Service staff prioritizes their incoming workloads and forwards investigations to OPM to be scheduled through our automated case management system, the Personnel Investigation Processing System (PIPS).

PIPS is a contemporary system that assists us in managing the flow and review of the casework, from the initial logging in and assignment of cases, to the online input of field investigation work, to the close-out to our agency clients and the tracking of agency adjudication decisions. As a sign of our teamwork and mutual concern, OPM began providing training to DSS staff in advance of our formal interagency Memorandum of Understanding earlier this year. All DSS investigative staff are expected to complete training ahead of the original schedule of June 30, and will be able to manage all new cases on PIPS. Through this configuration, DSS retains responsibility for their core workloads but strengthens their efficiency and cost effectiveness by using OPM's proven high volume automated processing system.

One of the other issues you asked OPM address, is the challenge of promoting reciprocity of security clearances. Although the decision to accept a clearance granted by another agency rests on the gaining agency, OPM is exploring options for increasing reciprocity with stakeholders. OPM is working to bring together the adjudicator community to promote understanding and common standards. In addition, OPM has taken significant steps to streamline access to current clearance information and make historic investigative files more readily accessible. Through our eClearance initiative, authorized agencies have on-line access to a subject's current clearance status literally at their fingertips. In addition, OPM is leading the effort to image investigative files in a format that will allow them to be delivered to an adjudicator's desktop electronically, rather than through the conventional, hardcopy process, saving significant time and handling.

Throughout this process, per the Director, OPM has made itself available to DOD Senior Officials, Congressional Staff and Stakeholders of the national security industrial sector to discuss the OPM/DSS joint efforts.

Mr. Chairman, this concludes my remarks. I would be happy to answer any questions the Committee may have.

Chairman TOM DAVIS. Thank you, Mr. Benowitz.

Ms. Anderson.

Ms. ANDERSON. Chairman Davis and members of the committee, I appreciate the opportunity to testify today regarding the improvements the Department of Defense [DOD] is making in the personnel security process and the status of the investigations backlog at the Defense Security Service. I have met with many industry representatives to discuss their concerns and to explain our ongoing initiatives and have received positive feedback. I believe that the improvement initiatives detailed in my prepared statement will resolve the fundamental problems that have plagued this program for several years, including the issues that industry will mention today.

First and foremost, I want to assure the committee members that we understand the impact from the inefficiencies that have been inherent in the past personnel security process. As you know, we have been working to identify and solve these fundamental problems and have been actively working to implement our solutions. Briefly, let me address the following: Reciprocity for industry, the investigations backlog, and our key initiatives to improve the personnel security process.

On reciprocity. Department of Defense implements reciprocity as defined in the National Industrial Security Program operating manual that identifies security requirements for industry. DOD ensures reciprocity through established security policies and procedures that are detailed in my statement. Basically, DOD accepts any previously granted clearance from any other Federal agency. Our policy of issuing interim clearances on a routine basis mitigates the lengthy processing of the final investigation and adjudication. Additionally, our policies permit industry to put their employees to work immediately once their company confirms the individual's clearance from their prior employer or agency. We understand our industry partners are working on special access and sensitive compartmented information programs may not currently experience the same benefit, and we are working with these communities to improve reciprocity. Our Joint Personnel Adjudication System will further improve this process and will virtually eliminate any time delay, since industry will be able to obtain clearance eligibility and access information online through this web-based system.

On the investigative backlog. Our backlogs in investigations from prior years has been nearly eliminated. While the overall work in process remains near 400,000 cases DOD-wide, DSS currently only has 86,700 prior year investigations in their inventory, of which 28,600 are industry cases, and many of these are in the hands of DSS' private sector contractors. Through an interim arrangement and agreement with the Office of Personnel Management [OPM], the current fiscal year investigations are being processed using OPM's case management system and they are being worked by DSS investigators. Due to the increase in demand for investigations, we expect our on-hand inventory to remain at this relatively high level until we are able to put more resources on task. To that end, DOD is currently working to increase the number of Federal investigators and we will continue to augment these resources with

private sector providers. It may well take up to 24 months to increase the capacity to that required level.

Next I will cover four initiatives to improve the process for personnel security investigations.

The first is the phased periodic reinvestigation for single scope background investigations. It is basically a two-phased approach where the second phase of field work is conducted only when significant potentially derogatory information is uncovered during the first phase. The pilot test and analysis show that substantial resources will be saved with a minimal loss of adjudicatively significant information. The personnel security working group of the National Security Council is currently considering this two-phased method for Government-wide implementation.

Our second process improvement is the Department of Defense automated continuing evaluation system. This automated assessment tool will allow the Department to identify issues of potential security concern. Currently in beta test, this system will be used initially to check our cleared population between reinvestigations, but ultimately will allow the Department to take an event-driven managed risk approach to reinvestigation, thereby eliminating purely periodic reinvestigations.

Third is DOD's adoption of OPM's Web-based personnel security questionnaire for Government-wide use. We expect to implement e-QIP within the Department as soon as possible, currently anticipated to be August 2004.

And, last, is the electronic reports for adjudication. The DOD Personnel Security Research Center is conducting a study on our behalf on how to develop criteria for electronic adjudication. The backbone of this effort will be an electronic report for adjudication that allows online review and adjudication DOD-wide. It will also allow for automated sorting and tracking of cases based on issue and complexity.

These initiatives will result in a personnel security process that is easier to use, more efficient, and take less time.

We were also asked to comment on the status of the transfer. As my colleague, Mr. Benowitz, has already mentioned, DOD stands ready to finalize any actions related to the transfer of the PSI function to OPM, should the Director of OPM choose to accept this function from the Department of Defense. The interim agreement in place with OPM allows for DOD to use their case management system and provides for agent training. The training has already begun and will be completed by the end of June 2004.

In conclusion, we have been working diligently for several years to meet the needs of our DOD customers, including industry. We owe a great deal to our industry partners who keep us informed of their concerns and upon whom we rely heavily for recommendations and feedback. Although slow in coming, I believe that significant progress has been made in improving the PSI process and that industry will soon benefit from our key initiatives. There is much more to accomplish, and we will continue to work with industry to ensure we understand and address their concerns as well as keep them informed of our progress on PSI process improvements.

Mr. Chairman, I ask for your continued patience, support, and assistance as we proceed to implement the improvements in the

PSI process. This concludes my testimony. I appreciate the opportunity to appear before you today and will answer any questions you may have. Thank you.

[The prepared statement of Ms. Anderson follows:]

Prepared Statement

Ms. Heather Anderson

Director, Strategic Integration and Acting Director, Security
Office of the Deputy Under Secretary of Defense, Counterintelligence and Security

Before the

Committee on Government Reform
U.S. House of Representatives

On

A Review of Security Clearance Backlog and Reciprocity Issues Plaguing Today's Government and Private Sector Workforce

May 6, 2004

Chairman Davis, Mr. Waxman, and members of the Committee on Government Reform, I am Heather Anderson, Director for Strategic Integration and Acting Director for Security, representing the office of Ms. Carol Haave, Deputy Under Secretary of Defense, Counterintelligence and Security, Department of Defense (DoD). I appreciate the opportunity to appear before you today to present testimony concerning the DoD security clearance backlog, reciprocity issues for Defense industry personnel, security clearance process improvements, and the status of the transfer of the personnel security investigations (PSI) function to the Office of Personnel Management (OPM).

The Department of Defense uses PSIs to ensure that only trustworthy and reliable individuals are granted access to classified information. The initial investigation provides assurance that a person has not demonstrated prior behavior that could be a security concern. The reinvestigation, conducted at specified time intervals after an initial investigation, is a periodic check designed to identify changes in behavior that may have occurred after the initial clearance was granted.

In the private sector, companies and their employees are processed for clearances under the auspices of the National Industrial Security Program (NISP). The NISP, created by Executive Order 12829, establishes a single, integrated cohesive system for safeguarding classified information held by industry. All Federal agencies participate in the NISP and most have delegated responsibility to the Secretary of Defense for the oversight of their contractors that require access to classified information. Only the Central Intelligence Agency, Department of Energy, and Nuclear Regulatory Commission have retained the authority and responsibility for their contractors for investigations, clearances, and program oversight. DoD, as the Executive Agent for the NISP, is responsible for industrial security policy that is conveyed to industry through the National Industrial Security Program Operating Manual (NISPOM).

The Department must have an affiliation with a private citizen before processing them for a personnel security clearance. For employees of DoD contractors, that relationship is established through the execution of a DoD Security Agreement, which is made a part of the contract with the company. Once the company has executed this agreement and is cleared, the company may process current employees or consultants for a background investigation if their duties will require access to classified information. The NISPOM also authorizes a contractor to submit a prospective employee for a clearance if that person has a written commitment for employment with a fixed date within the ensuing 180 days and the prospective employee has accepted the offer in writing.

Since 1986, DoD has routinely issued interim SECRET clearances to contractor employees who meet specified criteria based upon an initial review of their personnel security questionnaires. This review is conducted by the Defense Industrial Security Clearance Office (DISCO), the Defense Security Service (DSS) processing center for industry. DISCO reviews the information submitted on the clearance application, checks available databases to determine if the contractor

employee has a previous investigation that may be used to grant a clearance or, if there is no previous investigation, to determine if there is information that would indicate that it is not in the national interest to grant interim access without a completed investigation. If all factors are favorable, DISCO issues an interim clearance within 3 to 5 days of receipt of the request for investigation. If serious derogatory information is developed at any time during the course of the ensuing investigation, the interim clearance may be administratively withdrawn. The investigation, when completed, is sent to DISCO for final adjudication.

Approximately 85% of industry applicants are issued an interim clearance. For example, of the 152,059 requests for investigation from industry during FY03, approximately 85% of them were issued an interim clearance. An interim SECRET clearance authorizes access to SECRET information and most contractor employees can perform some functions with access to SECRET information, even if they ultimately require access to information of a higher level. DISCO also routinely issues interim TOP SECRET clearances when a favorable National Agency Check has been completed as part of the personnel security investigation (PSI).

DISCO has 76 trained adjudicators currently on board, an increase of 20 positions since September 30, 2003, and has been authorized an additional 28 adjudicative positions. DISCO adjudicators review the results of the investigation in accordance with the national adjudicative guidelines and issue the appropriate level of clearance. If DISCO is unable to make a determination that the issuance of a clearance is clearly consistent with the national interest, the case is referred to the Defense Office of Hearings and Appeals (DOHA) to provide the individual due process as required by Executive Order 10865. DOHA has also increased their adjudicative positions and has been able to significantly reduce the number of cases awaiting adjudication.

One of the key ongoing initiatives to improve PSI processing for industry is to expand DISCO's adjudicative role to serve as the nucleus for a single central adjudication facility (CAF) that will handle all adjudications for DoD cleared industry, to include trustworthiness and Sensitive Compartment Information (SCI) determinations. This plan, including the proposed structure, authorities, training, and resource details, should be finalized this calendar year.

DISCO electronically notifies industry when a clearance is issued and makes an entry in the DoD Joint Personnel Adjudication System (JPAS). JPAS is the DoD system of record for personnel security information for use by the DoD central adjudication facilities (CAFs), security managers, special security officers, and the DoD industrial security community and will ensure the standardization of core personnel security and adjudicative processes. JPAS achieved initial operating capability in February 2002. The inclusion of industry data in JPAS was initially impeded by the system configuration challenges of the DSS Case Control Management System (CCMS), resulting in repeated delays in exporting the information into JPAS. In September 2003 we were finally able to successfully import over 800,000 industrial personnel security clearance records from CCMS into JPAS. JPAS is now available to all of cleared industry security personnel and will become industry's system of record for clearance eligibility and access by September 2004. Currently, industry users are in the process of validating the data in the system to ensure that the information accurately depicts the security records of their cleared employees.

Use of JPAS will significantly reduce certain clearance processing actions. Once registered and online, companies will be responsible for maintaining their own security records and accomplishing transfers, reinstatements, and conversions of clearances for their employees. JPAS provides an automated view of an individual's clearance eligibility and access, and allows industry to immediately grant collateral access at the specified clearance level, record the access into JPAS or to terminate access, as appropriate. As of April 24, 2004, there were 4,377 industry JPAS users out of a population of approximately 11,500 cleared companies.

Currently, the NISPOM authorizes the transfer, conversion or reinstatement of a personnel security clearance (PCL) provided no more than 24 months has elapsed since the date of termination of the clearance. If the contractor is not using JPAS, the NISPOM requires that the contractor notify DISCO of the request for transfer, conversion or reinstatement and DISCO provides the authority to grant the employee access to classified information. However, in January 1999, the Director of Security issued a waiver, which is still in effect, to this NISPOM requirement allowing the contractor to verify from the losing contractor or government activity that the employee was cleared and the level of the clearance. Based upon this information, the contractor is authorized to grant immediate access to the employee at the verified clearance level. Industry has advised that they "are confident in estimating that tens of thousands of cleared employees have been able to begin new assignments with their clearances intact on day one." As a side benefit, DISCO is able to focus their adjudicative resources on issuing interim and final clearances rather than processing reinstatements and conversions.

It is important to note that the NISPOM defines reciprocity as follows:

> "Federal agencies that grant security clearances (TOP SECRET, SECRET, CONFIDENTIAL, Q or L) to their employees or their contractor employees are responsible for determining whether such employees have been previously cleared or investigated by the Federal Government. Any previously granted PCL that is based upon a current investigation of a scope that meets or exceeds that necessary for the clearance required, shall provide the basis for issuance of a new clearance without further investigation or adjudication unless significant derogatory information that was not previously adjudicated becomes known to the granting agency."

DoD ensures reciprocity through the transfer, reinstatement and conversion policies outlined above and by accepting background investigations and security clearance determinations from all other federal departments and agencies for access to equivalent levels and below. Based on our experience, the majority of industry reciprocity issues brought to our attention have involved access to special access programs (SAP), Sensitive Compartmented Information (SCI), or the practice on the part of other Federal agencies to review other government investigations and adjudications before granting access. SAP and SCI are programs requiring additional risk determinations prior to approving access and these access determinations are made by the services and intelligence agencies for military, civilian *and industry cases.*

Currently, funding for NISP contractor PSIs is provided through the Defense-wide Operating & Maintenance (O&M) appropriation. Based on a proposal to directly charge contractors for their PSIs, DoD conducted a study during FY 2003 to examine this alternative. That study concluded

that the Department would pay an additional 34% over its current costs for industry PSIs while directly shifting those costs to DoD procurements. Based upon that study, it was agreed that the current funding through O&M appropriations would continue. This approach requires a system that matches requirements to funding during the planning and budgeting process. In order to improve this process, JPAS will include a verification and validation module that will assist in predicting, verifying and validating future and continuing investigative requirements. Additionally, as part of the e-Acquisition initiative, DoD is working on details of a plan that will link investigative requirements to the contract specifications identified in the Contract Security Classification Specification (DD Form 254), and require contracting officer validation. This system will directly link more precise requirements to the budget process, yet allow for adjustments as necessary for unique contractual performance or modifications to contract.

FUTURE PLANS:

DoD is pleased that Congress supported and authorized the option to transfer the PSI function, including Defense Security Service (DSS) PSI employees to the Office of Personnel Management (OPM) in the National Defense Authorization Act for FY 2004. We understand that the Director of OPM has statutory discretion to accept or decline the full transfer of function from DoD, and that no final decision has been made at this time by the Director of OPM.

This initiative, as reflected in the President's Budget for FY 2004, was determined to offer the greatest opportunity to address the fundamental problems underlying the DoD PSI backlogs of prior years and the increasing demand for investigations throughout the entire Federal government. As the result of several studies, it was assessed that the consolidation of the PSI function would standardize investigations within the federal government, facilitate and expedite reciprocity and leverage public and private investigative resources to expand capacity.

Approximately 18 months ago DoD began to identify and address the actions necessary in anticipation of the potential transfer of the PSI function. One of our key objectives was to move the workforce to a common information system. With OPM'S agreement, we have moved forward to train the DSS personnel and to begin processing DoD investigations on OPM's Personnel Investigation Processing System (PIPS). By doing so, DoD takes immediate advantage of PIPS operating efficiencies and benefits investigators in particular by allowing them improved access to current information and improved insight into cases on a nationwide basis.

This interim agreement provides for case processing services and the use of the OPM computer system for the processing of DoD investigations. Currently, DSS investigative personnel are being trained on PIPS with the expectation that all DSS PSI personnel will be trained on the system by the end of June 2004. Those DSS personnel trained on PIPS have already begun to use the system to process DoD investigations. These interim efforts will ease the transition of operations should the final transfer occur and help focus our efforts on our ongoing e-government initiatives and other efforts to increase the capacity of the private sector to meet investigative demands. Additionally, DSS employees at the Personnel Investigations Center (PIC) are being retrained from scoping investigative leads to quality control services, as PIPS provides us with enhanced features with respect to investigative scoping.

One of the issues that has been of great concern to DoD and OPM has been inadequate investigative capacity to meet the demand for investigations government wide. To illustrate, DSS currently has approximately 1,200 investigators out of 1,855 PSI personnel. OPM's current investigative contract provider, United States Investigative Service (USIS), has approximately 2,900 investigators. Because some contractor investigators work for multiple private sector contractors, we estimate that the total investigative capacity of the federal workforce and private sector providers is approximately 5,300 in total. *Our assessment, based on current and predicted requirements, is that about 8,000 investigators are needed to meet federal investigative requirements.* We are moving forward on efforts to improve this situation. DSS is in the process of hiring an additional 200 investigators, and hopes to have these personnel on-board within 90 to 120 days. In addition, DSS has restructured their PSI organization to realign management to field (on-street) investigator positions. We understand that OPM also has efforts underway to add more private sector contract suppliers.

The timeliness of investigations is the measure most sensitive to any disturbance in the process, the measure that receives the most attention and is most disruptive to continuity of operations. We understand these concerns and have established the following investigative timelines: *95% of each case type* are to be completed as follows:

- *75 days* for initial investigations and reinvestigations for access to Secret and Confidential information,
- *120 days* for initial Top Secret, and
- *180 days* for Top Secret periodic reinvestigations,
- *With no case over a year old.*

Any future "backlog" within DoD will be defined as any case that exceeds these specified timeframes.

We understand that the "backlog" of old investigations pending completion at DSS and OPM has been an overriding concern for you. DoD has made great strides in eliminating this "backlog" of pending work. DSS investigative personnel have worked diligently to complete and close the oldest and most difficult investigations while beginning to process incoming Fiscal Year (FY) 2004 work using OPM's PIPS system. DSS personnel began actively working these cases, previously held at the CCMS gateway, in February 2004. Between October 2003 and to the present, DSS concentrated on completing all prior year work, which numbered over 250,000 investigations as of the beginning of fiscal year 2004. As of April 2004, DSS had successfully completed all but approximately 86,700 prior year investigations, of which 28,600 are for industry. At Attachment 1 is a chart that reflects pertinent statistics with respect to the status of industry investigations.

Through the phased transfer of DoD work to OPM's PIPS, we have eliminated the necessity to convert investigative files from one system to another and thus have avoided significant future delays in processing time. DSS predicts that all prior year (pre-FY 2004) work will be completed by the end of September 2004, and that no cases will be over one year old with the exception of some investigations on deployed personnel. DSS has also spent considerable effort identifying bottlenecks in the processing of investigations, and has determined that third party and overseas leads have been a major impediment to case completion times. Because the largest

backlog of records checks was at the FBI, DSS placed resources at the FBI to conduct and expedite the required records checks on DSS cases. As a result of these efforts, we expect the backlog of FBI checks to be current within the next few weeks.

The conduct of overseas leads traditionally has been accomplished by the military services. However, due to increased requirements on the military services in support of the war on terrorism, these competing demands diminished the support the military services were able to provide to conduct overseas work. To compensate, during March 2004, DSS began sending investigative personnel to Europe and to the Far East on an intermittent basis to conduct overseas leads. DSS is now developing a long-term plan to address the conduct of overseas investigations either by stationing personnel overseas or sending teams of investigators to specific locations on a 3-6 month rotational basis to conduct overseas investigations. DoD is also working with the State Department to update and refine the scope and sources for overseas investigations. The end result will be a more definitive and updated scope for overseas investigations on a government-wide basis. As part of this effort, we are also looking into database sources that may assist us in the conduct of overseas investigations.

Key Initiatives to improve the end to end PSI process:

Several key initiatives are underway within the Department of Defense to transform and significantly improve the end-to-end PSI process from identification of the requirement for an investigation through the final adjudication. These initiatives include:

Phased Periodic Reinvestigations:

In 2001, DoD began working on improvements to the single scope background investigation - periodic reinvestigation (SSBI-PR). As background, the Defense Personnel Security Research Center conducted initial research on the productivity of certain specified investigative sources in the SSBI-PR. Their research suggested the two-phased approach to the SSBI-PR, similar to medical screening where findings of initial tests determine if follow-up tests are required, was a valid alternative. During FY03 DoD conducted a pilot test of this phased approach. The results reflected that the phased SSBI-PR saves substantial resources with minimal loss of derogatory information. Recently, DoD presented the results of this pilot test to the Personnel Security Working Group (PSWG) under the Policy Coordinating Committee on Records Access and Information Security of the National Security Council (NSC). We are confident that the results will speak for themselves and that PSWG, representing the entire security community, and the National Security Council (NSC), will approve the Phased PR as part of the national investigative standards.

Automated Continuing Evaluation System (ACES):

ACES, an automated assessment tool, is designed to identify issues of security concern on cleared personnel between the specified periodic reinvestigations (5 years for Top Secret access, 10 years for Secret, and 15 years for Confidential). Through ACES, and with the consent of the individual, specified databases will be searched to identify information that assists in the

evaluation of cleared individuals in order to determine their suitability for continued access to classified information. ACES will automatically identify and schedule cleared personnel for a series of database checks that include: credit reports, FBI criminal history, Treasury large currency transaction filings, foreign travel, and real estate ownership records. The report produced by the database will be electronically forwarded to the appropriate DoD CAF for review and adjudication, as necessary. As additional appropriate data sources are identified or become available, DoD will conduct the necessary research, testing, and programming to include them as part of ACES.

Initially, ACES checks will be conducted on personnel holding TS/SCI clearances at the mid-point between their reinvestigation cycle of five (5) years. However, within the next few years, DoD will conduct an annual ACES check on individuals holding all levels of clearance. Eventually, it is hoped that ACES will provide a means to eliminate the periodicity of reinvestigations and transform the personnel security process into a proactive, risk-managed process.

e-QIP

As an active participant and advocate for the e-Government/e-Clearance initiative, DoD will transition this fiscal year from the electronic personnel security questionnaire (EPSQ) system to e-QIP, the on-line, web-based e-clearance investigation request form developed by OPM. Thereafter, DoD components will be required to use eQIP for submitting investigative requests. Verification and validation of the request will be accomplished up front through the JPAS interface. An essential and important part of this effort includes the pre-population of e-QIP from information on an individual's most recent EPSQ, where available. Data submitted through this electronic submission will remain on e-QIP and can be revised and updated by these individuals on-line.

Electronic Report for Adjudication (e-RFA)

The DoD Personnel Security Research Center is also conducting a study to develop criteria for *electronic adjudication*, using the electronic Report for Adjudication (e-RFA) as the foundation. DoD is working with OPM to expedite the e-RFA that provides for the electronic submission of the investigative report to the adjudicative facilities to allow for on-line review and adjudication, except in those instances when manual processing may be required due to significantly derogatory information. We estimate that e-RFA will reduce the overall processing time for adjudication and we are looking forward to implementation of this improvement.

CONCLUSION:

We have been working diligently over the past several years to meet the needs of our DoD customers, including industry. We owe a great deal to our industry partners who keep us informed of their concerns and upon whom we rely heavily for recommendations and feedback.

Although slow in coming, I believe that significant progress has been made in improving the PSI process and that industry will soon benefit from our key initiatives. There is much more to be accomplished, and we will continue to work with industry to ensure we understand and address their concerns. We will continue our outreach to industry to keep them informed of our progress on PSI process improvements.

Mr. Chairman, I ask for your continued patience, support and assistance as we proceed to implement the changes that are required to improve the end-to-end PSI process. I appreciate the opportunity to appear before this Committee today and I will be pleased to answer any questions that you may have at this time.

Attachment 1

Industry PSIs

Prior Years	Total Number Submitted	% Completed within target days	% Completed within 360 days*
NACLCs (75 days)			
FY01	77,113	15%	76%
FY02	97,419	50%	89%
FY03	102,783	34%	97%
SSBIs (120 Days)			
FY01	11,662	7%	54%
FY02	17,751	22%	86%
FY03	21,905	15%	99%
TS PRs (180 days)			
FY01	16,566	8%	49%
FY02	23,272	29%	74%
FY03	23,029	18%	87%

*%'s pertain to DSS closings only - for cases received in the FY

FY04 through April 24	Total Number Complete Packages Submitted	% scheduled to field
SSBIs and SIIs	7,083	41%
TS PRs	5,260	16%
NACLCs	32,862	27%
Total	45,205	

Improvement Targets	Total Number Projected to be Submitted	% Completed within target days	% Completed within 360 days*

NACLCs (75 days)			
FY04	117,429	50%	98%
FY05	119,778	80%	100%
FY06 and out	122,173	95%	100%
SSBIs (120 Days)			
FY04	28,374	50%	98%
FY05	29,793	80%	100%
FY06 and out	31,282	95%	100%
TS PRs (180 days)			
FY04	23,029	50%	98%
FY05	24,200	80%	100%
FY06 and out	42,200	95%	100%

NACLC: National Agency Check with Local Agency Checks and Credit Check
Initial and reinvestigation for access to Secret and Confidential information

SSBI: Single-scope Background Investigation
Initial investigation for access to Top Secret information

TS PR: Top Secret Periodic Reinvestigation
Reinvestigation for access to Top Secret information

Chairman TOM DAVIS. Thank you very much.

Mr. Leonard.

Mr. LEONARD. Chairman Davis, members of the committee, thanks very much for the opportunity to be here with you this morning. As Director of the Information Security Oversight Office, one of my responsibilities is to oversee Government agency actions with respect to the National Industrial Security Program [NISP]. In addition, I serve as the Chair of the National Industrial Security Program Policy Advisory Committee [NISPPAC], which is comprised of both Government and industry representatives. The NISPPAC advises me on all matters concerning the policies of the NISP and serves as a forum for discussing policy issues.

The overall framework for the NISP is set forth in Executive Order 12829. This Presidential directive recognizes the obvious imperative to ensure that classified information in the hands of industry is properly safeguarded. However, what is equally significant is its recognition that our industrial security program must also promote the economic and technological interests of the United States. As such, an essential element of the NISP is its acknowledgement that redundant, overlapping, or unnecessary requirements imposed upon industry can imperil national security as readily as can the improper safeguarding of classified information. A common cause of unnecessary requirements is the inability of agencies to reciprocally honor a similar action taken by another agency, such as a personnel security investigation or a personnel security clearance involving the same individual—a practice commonly referred to as reciprocity.

Before the creation of the NISP, each agency had its own individual industrial security program. Each program had processes that were unique. The NISP has helped to create an atmosphere of cooperation for both Government and industry by eliminating duplicative processes. More than 10 years after its inception it would be hard to imagine an environment without the NISP. However, notwithstanding past successes, today's challenges require constant attention and effort from participating agencies in order for the NISP to achieve its full potential in promoting the economic and technological interests of our Nation. This is especially so in recognizing industry's critical role both in the current war efforts as well as many of the transformational activities currently underway in much of the Federal Government. In this regard, agencies' inability to accomplish actions such as clearing defenses contractor employees in a prompt manner, or to honor reciprocally a similar action by another Government agency has a significant and deleterious impact upon cleared industry's capability to support their Government customers.

Oftentimes, agencies cite fear of accepting an unknown potential security risk as a basis for not embracing reciprocity. I know of no empirical basis to support a claim that reciprocity reduces security or increases risk. Instead, I contend that the failure to achieve full reciprocity can actually increase the overall security risk for the Nation. Lack of reciprocity needlessly distracts limited resources that can be devoted to the current unacceptable delays in processing new, initial clearance requests, as well as the backlog periodic reinvestigations.

In addition, reluctance on the part of Government agencies to forego some agency prerogatives and fully embrace all the tenets of the NISP, especially reciprocity, hampers industry's ability to recruit and retain the best and the brightest in their disciplines as well as its capability to rapidly deploy and field the latest technology when performing on classified contracts. As a result, contractors are hampered in putting forth the best conceivable efforts in both cost and capability in supporting their Government customers' needs. The Government effectively ends up with less for more.

In order to assist in reducing clearance delays in industry, my office, through the NISPPAC, has served as a forum for industry to provide their concerns and recommendations to the Government's current working groups addressing personnel security clearances. Even more specifically, we have recently initiated a renewed effort to have NISPPAC issue and publicize a clear articulation of what reciprocity is, and is not, with enough specificity and substance that industry can hold Government agencies accountable for their actions in this area. I am pleased to report that we have succeeded in garnering senior level support within NISP Government agencies for these efforts and I anticipate formal promulgation within a matter of weeks. This declaration is not a silver bullet. However, it should allow contractors who experience reluctance on the part of a Government program or contract office to honor reciprocally a clearance action by another Government agency to seek immediate redress.

Again, thank you for inviting me here today, Mr. Chairman. I would be happy to answer any questions.

[The prepared statement of Mr. Leonard follows:]

FORMAL STATEMENT

J. William Leonard
Director, Information Security Oversight Office
National Archives and Records Administration
before the
Committee on Government Reform
U.S. House of Representatives
May 6, 2004

Chairman Davis, Mr. Waxman, and members of the Committee on Government Reform, I wish to thank you for holding this hearing on security clearance backlogs and reciprocity issues for defense industry personnel and for inviting me to testify today. As Director of the Information Security Oversight Office, one of my responsibilities is to oversee Government agency actions with respect to the National Industrial Security Program (NISP) in order to ensure compliance with established policy.

The overall framework for the NISP is set forth in Executive Order 12829, as amended (the Order). This Presidential directive recognizes the obvious imperative to ensure that classified information in the hands of industry is properly safeguarded. However, what is equally significant is its recognition that our industrial security program must also promote the economic and technological interests of the United States. As such, an essential element of the NISP is its acknowledgment that redundant, overlapping, or

unnecessary requirements imposed upon industry can imperil national security as readily as can the improper safeguarding of classified information. A common cause of unnecessary requirements is the inability of agencies to reciprocally honor a similar action taker by another agency, such as a personnel security investigation or a personnel security clearance involving the same individual – a practice commonly referred to as reciprocity.

Pursuant to the Order there are four signatories to the National Industrial Security Program: the Department of Defense (DoD), the Central Intelligence Agency (CIA), Department of Energy (DOE), and the Nuclear Regulatory Commission (NRC). In addition, all other Federal agencies that engage contractors on a classified basis are required to assume the status of User Agencies.

The Order assigns to the Secretary of Defense the responsibility to serve as the Executive Agent for the NISP. Furthermore, the Director of Central Intelligence (DCI) retains authority over access to intelligence sources and methods, including Sensitive Compartmented Information (SCI). Likewise, both the Secretary of Energy and the Chairman of the NRC retain authority over access to information under their respective programs classified under the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 et seq.).

In addition to overseeing Government agency actions to implement the Order, as ISOO Director, I serve as Chair of the National Industrial Security Program Policy Advisory Committee (NISPPAC), which is comprised of both Government and industry representatives. The NISPPAC advises me on all matters concerning the policies of the NISP, including recommending changes to those policies. The NISPPAC also serves as a forum for discussing policy issues in dispute.

Before the creation of the NISP in 1992, each agency had its own individual industrial security program. Each program had processes that were unique. The NISP has helped to create an atmosphere of cooperation for both Government and industry by eliminating many duplicative processes. More than ten years after its inception it would be hard to imagine an environment without the NISP. However, notwithstanding past successes, today's challenges require constant attention and effort from participating agencies in order for the NISP to achieve its full potential in promoting the economic and technological interests of our nation, especially recognizing industry's critical role in both the current war efforts as well as many of the "transformation" activities currently underway in much of the Federal Government. Inevitably, the leveraging of technology and services from the private sector are an integral part of these efforts.

Often, NISP participants refer to the program as a "partnership" between Government and industry. However, it is more than that - it is also a legally binding contractual relationship. As with all contracts, both parties commit to do certain things. Industry, of

course, agrees to protect classified information. The Government, in turn, agrees to do certain things as well. In fact, in many instances, Government action is a prerequisite for contractor action.

For example, contractors cannot provide an employee with access to classified information until the Government clears that individual. Yet, with respect to promoting our nation's economic and technological interests, agencies' inability to accomplish this and other prerequisites in a prompt manner or to honor reciprocally a similar action by another Government agency, has a significant and deleterious impact upon cleared industry's capability to support their Government customers.

Oftentimes, agencies cite fear of accepting an unknown potential security risk as the basis for not embracing reciprocity. I know of no empirical basis to support a claim that reciprocity reduces security or increases risk; instead, I contend that the failure to achieve full reciprocity can actually increase the overall security risk for the nation. First, needlessly requiring and reviewing security forms and investigative files, and oftentimes requesting duplicative investigations, all for individuals who have already been deemed trustworthy by another Government agency, needlessly distracts limited resources that can be devoted to the current unacceptable delays in processing new, initial clearance requests. Second, this practice has also contributed to a backlog in periodic reinvestigations. Ironically, the proven risk does not lie with individuals who transfer from Government to industry, industry to Government, or company to company and who

undergo the additional vetting process inherent to being interviewed and hired for a new job. Rather, the proven risk often rests with individuals who might be viewed as being in a "career rut." Currently, such individuals are oftentimes experiencing prolonged delays in undergoing a periodic reinvestigation.

In addition, reluctance on the part of Government agencies to forego some "agency prerogatives" and fully embrace all the tenets of the NISP, especially reciprocity, hampers industry's ability to recruit and retain the best and the brightest in their disciplines as well as its capability to rapidly develop and field the latest technology when performing on classified contracts. As a result of this inability to achieve and maintain the NISP's full potential, contractors are hampered in putting forth the best conceivable efforts in both cost and capability in supporting their Government customers' needs. As such, the Government effectively ends up with less for more.

In order to assist in reducing clearance delays in industry, my office, through the NISPPAC, has served as a forum for industry to provide their concerns and recommendations to the Government's current working groups addressing personnel security clearances – specifically a group under the auspices of the National Security Council as well as a separate group under the auspices of the DCI's Special Security Center. Our goal is to assist in establishing an ongoing dialogue to ensure industry's unique circumstances are understood as Government agencies wrestle with the many longstanding issues that plague the personnel security arena – recognizing that overall

responsibility for personnel security policy is beyond the immediate purview of my office.

Even more immediate, we have recently initiated a renewed effort by the NISP signatories to implement near-term solutions to the issue of reciprocity within industry. The goal is to have NISPPAC issue and publicize a clear articulation of what reciprocity is (and is not) with enough specificity and substance that industry can hold Government agencies accountable for their actions in this area. I am pleased to report that we have succeeded in garnering senior level support for these efforts and anticipate formal promulgation within a matter of weeks. This declaration is not a silver bullet. However, it should allow contractors who experience failure on the part of a Government program or contract office to honor reciprocally a clearance action by another Government agency to seek immediate redress.

Many thousands of individuals within Government and industry are responsible for the progress made to date in implementing the NISP. There is more that needs to be done, and ISOO will be working closely with our partners in industry and Government in building upon a much needed renewed commitment to the NISP's original goals and objectives.

Again, I thank you for inviting me here today, Mr. Chairman, and I would be happy to answer any questions that you or the Committee might have.

Chairman TOM DAVIS. Thank you very much.

In 1981, GAO issued a report citing the national security threat posed by the backlog as well as the contract cost overruns caused by the delay, and they estimated at that point it was about $1 billion a year. Since that time my son has been born, he is graduating from college this year, and the Federal Government is in the same boat, in fact, the backlog has increased during that time. Let me start with you, Ms. Anderson, why is the Federal Government in relatively the same boat with the same issues 23 years later? I know you were not old enough to work for the Government 23 years ago, so you were not part of it then but you are there now. [Laughter.]

Ms. ANDERSON. Thank you, sir. The Department of Defense has taken a really hard look, certainly within our purview, at the end process. One of the fundamental problems with security clearances, and it really was highlighted after September 11, is that you need people immediately. We are in the business of being agile and to have a defined process that requires you to go through a lengthy vetting is inherently mismatched with the immediate need. This is compounded by the belief, I believe historically, that this year was always going to be the peak year.

One of the problems is we have looked at this series of requirements year over year. One of the things we are finally going to bite the bullet on is to actually verify the requirement as it is submitted. It is the one place where we will have the opportunity to actually get conformed data. We are going to introduce both macro economic models and bottom-up models to actually try to get the projection correct.

Chairman TOM DAVIS. So you said you are afraid to staff up because you may not need the people in the out years?

Ms. ANDERSON. If you go back into a lot of the responses historically, there has been some of that indicated. One of the reasons that we believe that a partnership between Federal investigators and contractor augmentation is actually to allow more flexibility with that number. But who is kidding who? The number of clearances has not gone down in quite a while and we seem to move more and more in that direction.

Chairman TOM DAVIS. Well, understand this, somebody with a security clearance, we are paying them a lot more than taxpayers ought to be paying because there are so few people that are eligible to do it. We cannot get work done. Taxpayers are paying more money. DOD is going to come up here for another $25 billion in a supplemental this year. It was $1 billion in 1981, it is several billion dollars it is costing taxpayers today. My opinion is that nobody is really paying attention. Everybody is shuffling things back and forth. This is a huge problem. It is costing us billions of dollars and we are sitting here with OPM and pointing back and forth. Congress, we can pass a very strong bill, we take it away from both of you. I am not sure how we handle this, but it is costing a lot of money at this point and it is jeopardizing security. I understand how we got there. What are we going to do about it?

Ms. ANDERSON. Interestingly enough, as I alluded to in my verbal statement and in my written testimony, we are in the process of putting more investigators on the street. The strategic part-

nership between OPM and DOD, their Request for Proposal that is being evaluated now, the DSS PSI program has reengineered their organizational structure and their business processes to allow more of their people to be on the street doing investigations. We recognize that is not enough. Also understand that part of the inherent lag is it takes a good 6 months to train an investigator. So while we are recruiting these people now, they will not be up to full productivity for probably at least 6 months.

Chairman TOM DAVIS. We have given additional Civil Service authority to the Department of Defense. We passed this last year. A tough vote for a lot of us. OK? You can bring people who used to do this back into Government. You can do these kind of things and you do not have to retrain them.

Ms. ANDERSON. Correct, sir. We believe that organizationally, and I will defer to my colleagues from OPM to confirm this, we believe that we have tapped out the number of people who were prior investigators coming back to do this work.

Chairman TOM DAVIS. Have you brought prior investigators back in? Do you know how many?

Ms. ANDERSON. I do not have the facts with me.

Chairman TOM DAVIS. Can you get that to us?

Ms. ANDERSON. Yes. But that is primarily what the contractor investigators, that is what their resource pool is.

Chairman TOM DAVIS. OK. From the testimony you would think industry personnel were able to get the clearances they need quickly. You said contractor companies can apply for a clearance up to 180 days in advance of an employee starting work, they can obtain an interim secret clearance within 3 to 5 days of applying for a clearance, they can nearly automatically transfer a clearance when a worker moves from one job to another. But we continue to receive complaints, the GAO has confirmed it, Mr. Leonard says the same thing, that the process is not working. Now you recognize the process is broken?

Ms. ANDERSON. Yes, sir.

Chairman TOM DAVIS. How about you, Mr. Benowitz, do you recognize the process is broken, or is everything just fine over there?

Mr. BENOWITZ. Mr. Chairman, we believe the process is one that needs substantial improvement. Director James is as concerned with national security as DOD, and the contractors who will testify later today. My colleague, Ms. Anderson, has spoken of some of the steps we are taking. My view of the RFP that OPM has under evaluation right now is that we will begin to see substantial increases in the number of contract investigators on the streets trained and doing the work about 6 months after the contracts are awarded. Our intent there, if possible, is to make multiple awards to multiple firms so that we can increase that contractor base.

Chairman TOM DAVIS. Let me just make one point before I yield. There is an article yesterday in Government Executive.Com that basically talks about you are holding off on the plan to absorb the unit of DOD. This is a move that some experts had thought might speed up the backlog security clearance process. You had planned last year to take over Defense Security Services, now an OPM official said the agency decided not to bring the unit under its um-

brella, that the DSS business practices were not up to the standard we had hoped for.

You have discussed the transfer of the investigative functions from DOD to OPM. But it appears that DOD views this transfer as a complete divestiture and OPM views it more as a partnership. I guess the question is, which one is it? In addition, as I said, yesterday OPM announced it would not accept the transfer this year. Why was this decision made? And does DOD have a backup plan for dealing with the backlog?

Mr. BENOWITZ. Mr. Chairman, when the Director of OPM and the Secretary of Defense agreed to explore such a transfer of function, which began before the legislation was enacted, we began sharing information with each other. We determined subsequent to that that this should be staged. The first stage, as I indicated today, was that we have given DOD access to our online case management system, PIPS, that their staff will be fully trained by the end of June, and they will be managing all of their new caseload on this system. We began this in advance of a formal agreement that was signed in February of this year. We will be conducting evaluations of the productivity of the DSS staff in June and September when they will have had an opportunity to perform their work under PIPS, and we are——

Chairman TOM DAVIS. But everybody is still studying everything. Is that what I take away from this, that we are still studying this and it is going to take a few more months?

Mr. BENOWITZ. I expect that we will have information available for our final evaluation by the end of the fiscal year.

Chairman TOM DAVIS. So that is October. You are still studying it and hope to get something.

Ms. Anderson, can you give us any encouragement here? Again, just to go back to the report, in 1981 this was identified in the report, and we hope to get some information by the end of the fiscal year and maybe get the top honchos together. Can you give me any encouragement here?

Ms. ANDERSON. Sir, in reference to your earlier question about DOD's plan while we discuss the transfer function, the Department of Defense is processing its current caseload. A significant proportion of that is already on OPM's system and is being worked by the DSS investigators. OPM is processing the military accessions and the civil populations, as they have the civilians for a number of years now. The industry cases, in particular, are being worked by the DSS agents off of the OPM system. We can work in this configuration for a length of time, an indeterminant length of time under the current agreement with OPM. So the cases are being worked. We are tightening down as far as trying to improve the efficiencies, improve the reporting, improve the insight into the process while we look at and reexamine all of our policies and procedures to make sure that we are the most efficient organization we can be.

Chairman TOM DAVIS. Do we have a chart blown up on this? Let me ask our representative from GAO, what do you think of all of this? I have a chart I want to put up here that talks about all the rigmarole we are going through to get a clearance now in this sys-

tem. We are just going to have more of a backlog if we keep going. What do you think, Mr. Wilshusen?

Mr. WILSHUSEN. Looks like a rather elaborate chart. [Laughter.]

Chairman TOM DAVIS. This chart is actually simplified from what really happens.

Mr. WILSHUSEN. What this chart appears to show, Mr. Chairman, is that there are a number of agencies involved in determining what the requirements for clearances are and that they appear to be going over to OPM and DSS in terms of having the investigations performed. It looks as though that as part of that, the chart shows some of the activities that both OPM and DSS have to conduct and the volume of pages of information they review.

Chairman TOM DAVIS. They are the bottlenecks though basically, are they not?

Mr. WILSHUSEN. There are a few bottlenecks, yes, sir. And the chart shows each of the three processes of determining the requirements, the investigation stage as well as adjudication stage.

Chairman TOM DAVIS. Do you hear any encouragement in what we are hearing today about any immediate relief? Or do we just say to the contractors and taxpayers you are just going to have to pay a little more because the people that we put in these positions are still studying this?

Mr. WILSHUSEN. I think in terms of some of the initiatives that DOD is considering, some of them do hold promise. One of the recommendations that we may be making as part of our draft report is that they continue to look at those initiatives to see if they are feasible and implementable.

Chairman TOM DAVIS. That is long term. What do you do short term to bring this thing down for the guy who has been waiting a year for a clearance and still does not have a job, and the task needs to be performed for the country?

Mr. WILSHUSEN. Well, one of the things that DOD has done is issued interim clearances. But there are some problems in terms of interim clearances in that often they do not allow access to certain types of information or for certain programs. In addition, there is also an inherent security risk in issuing an interim clearance, because you are allowing an individual access to classified information without going the full range of investigation over that individual which could yield some derogatory information.

Chairman TOM DAVIS. Essentially, this is manpower-driven, is it not?

Mr. WILSHUSEN. No question about it.

Chairman TOM DAVIS. And we do not have enough people on it.

Mr. WILSHUSEN. The underlying reason for many of these things and the No. 1 challenge is for them to match the size of their adjudicative and investigative work forces with their workload.

Chairman TOM DAVIS. And is it not cheaper to have people at the front end getting these clearances done than paying more at the back end because we do not have enough people to do it and so we overpay? Does that make sense?

Mr. WILSHUSEN. Well, it does indeed. It is very important to make sure that process is done in a timely and effective manner.

Chairman TOM DAVIS. Yes. It is a people problem. I do not think it is a budget issue.

Ms. Watson, your questions, then we will get Mr. Schrock, and then Mr. Moran.

Ms. WATSON. I want to move away from the backlog and into the responsibilities and accountability of the Department of Defense Security Services. I will address my questions to Ms. Heather Anderson, Acting Deputy Director. Once you are able to complete the process, background check and certifying, clearing this person, who has the oversight? Who is accountable? Who then holds the control of this employee after this employee goes into the investigative mode? In reading from your statement, you are suggesting that the responsibility for conducting leads overseas will be with the Department of Security Services. Is that correct?

Ms. ANDERSON. Currently, the overseas leads are executed by the military services. One of the things that we have taken an initiative on is to augment the military services, who are rather busy around the globe, especially in certain theaters, and put Defense Security Service agents who are trained investigators to run those leads in their place in order to reduce the number of longstanding cases and in order to process cases in general.

Ms. WATSON. You say in your statement, "To compensate, during March 2004, DSS began sending investigative personnel to Europe and to the Far East on an intermittent basis to conduct overseas leads." And that DSS is now developing a long-term plan to address the conduct of overseas investigations.

Ms. ANDERSON. What it is, as part of our national standards there are certain leads, like neighborhood checks, subject interviews, that are run. In cases in particular where the subject is overseas, we want an investigator to be there to do the subject interview. Historically, those leads have been run by the military services and then the results of those leads written up and returned to Defense Security Service for inclusion in the reports for adjudication. What we are considering is whether or not it would be more efficient and more practical to have either a series of travel assignments overseas or a standing group of investigators overseas to service those leads. It is not so much——

Ms. WATSON. If I might interrupt you for a minute. You are saying that you have already done this, you have started.

Ms. ANDERSON. Yes.

Ms. WATSON. That, at least, is what your written statement says.

Ms. ANDERSON. Right. They were authorized to do a pilot to look at the feasibility and utility of it. The initial results from that pilot were very encouraging and the services welcome the opportunity for DSS to run those leads. So now we are working through how we implement it and substantiate it.

Ms. WATSON. You say in your written statement, "DOD is also working with the State Department to update and refine the scope and sources of overseas investigations." Who is responsible for those investigators, interrogators, the security forces that you have sent overseas to investigate leads?

Ms. ANDERSON. In the case where we are talking about the investigators from Defense Security Service, they are under the cognizance of the Director of Defense Security Service. We have not sent them into areas where there is conflict. The two pilot programs where there was the largest body of leads outstanding were

in the Pacific theater, specifically Korea and Japan, and so we have teams there, and also in the European theater, particularly in Germany and the U.K.

Ms. WATSON. All right. Let me get directly to where I am going. I see that you are involved with intelligence. Would your department, would you with the people under you have anything to do with the interrogators that would have been sent to Iraq as contract employees to do the investigation, interrogations, questioning, etc?

Ms. ANDERSON. Under the Under Secretary of Defense for Intelligence, we do have oversight for a large piece of the service intelligence organizations. More specifically to your question with regard to contractor investigators, the investigations on those personnel, the background investigations on those personnel may very well have been done by Defense Security Service.

Ms. WATSON. By your unit?

Ms. ANDERSON. But not the unit that was overseas necessarily. For the most part, they would have been United States.

Ms. WATSON. Well who would have done that? Who do they answer to? Who oversees them? Who has a responsibility for them? I am trying to follow a trail. We have a very elaborate chart here, very graphically done, artistically done, but I am trying to follow a trail and I cannot get there from here.

Ms. ANDERSON. I will start from the beginning. If, in this case, the Army were going to let a contract for services with a contractor provider, they would let the contract, depending on what the clearance level required, so let us assume it is secret, they are going to write the contract with security requirements in it. The contractor then, as part of the execution at the stand-up of that contract, will put in their employees for background investigations. Those background investigations would be sponsored under this because of the NISPAM, the Industrial Security program, they will be processed by DSS, they are funded for centrally because there is a number of benefits to that, the results of an investigation would go to the Defense Industrial Security Clearance Office for adjudication. If there were derogatory issues that needed to be determined from a statement of reasons or from an eligibility, it may very well go to the Defense Office of Hearings and Appeals. They will render a determination of eligibility. That is then returned to the contractor who is told, if it is favorable, that they may access the person to secret information. The oversight of the execution of a contract belongs to the entity that let the contract.

Ms. WATSON. And that is?

Ms. ANDERSON. In this case, you are talking about the Army. We have contracts for Navy. I have people on my staff where they are contractor support, we sponsor them and we are responsible for the oversight. The security manager from the company also has some responsibility to make sure that person is adequately aware of their responsibilities and duties as a cleared person. Does that help answer your question? Probably not from the look.

Ms. WATSON. No.

Chairman TOM DAVIS. OK. Thank you. Followup?

Ms. WATSON. Can they give orders to our troops, your contractees?

Ms. ANDERSON. Not normally, ma'am.

Ms. WATSON. Thank you.

Chairman TOM DAVIS. OK. Mr. Schrock.

Mr. SCHROCK. Mr. Chairman, I am so confused at this point I am not sure what I should ask. I was doing great until I got this thing. [Laughter.]

I do not know if anybody here created this, but I sure would like to get into that person's mind.

Chairman TOM DAVIS. I think it came from DOD. Ms. Anderson, not to point fingers here, but you are the DOD rep.

Mr. SCHROCK. I do not have a clue what this means. All these nice little lightening strikes and all that, there are going to be lightening strikes all right, but it is not going to be on this chart. This is nonsense, really. I heard Mr. Wilshusen say, as I understood him, there is no plan to get rid of the backlog. I heard Mr. Benowitz say that there is an RFP out there and if it gets addressed or awarded, it is going to take 6 months to get it in place. And I heard Ms. Anderson say there are 180,000 folks in DOD backlogged, 24 months to increase capacity, and for us to be patient and that we have to be agile. Folks, we are not agile, we are comatose right now. I do not know what the answer is to this. Chairman Davis is going to have a grandson graduating from college before this gets done. [Laughter.]

I know it sounds funny, but this is ridiculous. At some point we have to get this thing resolved. I am wondering to what extent are field agents held responsible, those in the field, to get productivity done. And study, study, study, gosh, that is all we do. The pillars of this Government stand on studies. I feel certain we have studied this thing to death. At what point do we knock off the studies and start putting pen to paper and get this work done. Who is being held accountable for this? And how many agencies are doing it? Mr. Moran, Mr. Davis, and I have thousands and thousands of constituents who are negatively impacted by the inactivity in all this stuff. At some point the rubber has to meet the road. How do we get this resolved not 6 months, not 24 months, but tomorrow. How do we get this resolved? The silence is deafening.

Chairman TOM DAVIS. GAO, what would you recommend?

Mr. SCHROCK. Yes, what do you recommend?

Chairman TOM DAVIS. The GAO is the neutral party here.

Mr. WILSHUSEN. Indeed, there are a number of actions that DOD can do to address this issue. First and foremost, as we recommended in our February report, they need to match the size of their investigative and adjudicative work forces with their respective workloads. And closely attendant to that is developing the capability and improving their models for projecting what their future requirements are going to be. Until you know what your requirements are—in fact, at present, DOD has not been able to even determine what their full backlog is DOD-wide, not just industry contractors but DOD-wide, what their full backlog is. That is definitely a first step.

Chairman TOM DAVIS. Would the gentleman yield. Let me just ask, statutorily, what could we do? We have a defense authorization bill coming up before the House. We are obviously involved in that from this committee's perspective. What could you do very

quickly to put some mandates on this and make it move over the short term? If you want, we will let you get back to us.

Mr. WILSHUSEN. Yes, Mr. Chairman, we will do so.

Chairman TOM DAVIS. But I think we are as frustrated as taxpayers are, as contractors are, as people who are awaiting clearances are in terms of how we get out of this.

Mr. SCHROCK. Mr. Chairman, may I?

Chairman TOM DAVIS. It is your time.

Mr. SCHROCK. May I give you an example of how ludicrous this is. I several months ago hired a young man who had been in the nuclear navy, probably had the highest clearance any human being on the face of the Earth could have, but he left the Navy 1 day and came to work with me the next day and, suddenly, his clearance was not any good. Now what happened to him overnight to make him a risk? And he had to go through this whole process again. That is nonsense.

Mr. WILSHUSEN. Yes, sir, that is one of the problems.

Mr. SCHROCK. Why is that the case? Can DOD answer why that is the case?

Ms. ANDERSON. Sir, your background investigations and your adjudications are not done by the Department of Defense. Within the Department of Defense, we are taking the steps to make sure that does not happen. Under our Joint Personnel Adjudication system, we are specifically making sure that the entities that are the gaining and losing entities have flexibility, the gaining entity in particular, whether that is a contractor, a military service, any organization within our affiliation structure, that as soon as they have an obligation document, so in your case, when your employee agreed that he was going to come to work for you, which is generally just by tradition sometimes a few weeks if not a month in advance, at that point your security manager could actually identify the association, at that point you are a part owner, as it were, in that process. So if an investigation were ongoing, or if you needed to access that person, we make sure that it does not fall through the cracks. We are devolving that responsibility down to the lowest level because they are generally the ones that know what is going on. That is exactly why we have taken that step. But with regard to your specific example, I am afraid I do not have a good answer.

Mr. LEONARD. If I could add, Congressman.

Mr. SCHROCK. Please, Mr. Leonard.

Mr. LEONARD. You are absolutely right, it is ludicrous. And it has been the policy for over 10 years now that situation should not occur. There is a long history in terms of agency prerogatives and this and that. One of the things that I am somewhat optimistic on, and I temper that optimism with a lot of reality, but I am optimistic in terms of I personally within the past several months have visited with all the senior security officials of the NIST signatories, at least dealing with industry, and everyone recognizes that reciprocity is just plain good Government and makes good sense. But today, it makes even better sense when there are so many perturbations and strains on a personnel security process. I got a commitment from all four senior security officials to convene a working group, which we have done within the past month.

That working group has offered up a declaration, a specific articulation of exactly what reciprocity is, that I anticipate that we shall be able to promulgate hopefully within a matter of weeks. This will be publicly disseminated. All of industry will get it. They will know exactly what the standards are. They will know precisely when a Government agency is failing to comply with it. And part and parcel of this will be a single point of contact with every agency in terms of when a program office fails to comply who do I go to in DOD, CIA, DOE, or whatever, with a copy to my office and we will followup on that. Now this is not a silver bullet. It is not going to address all the issues. But at least this will get us away from wasting resources on people we have already determined to be trustworthy and reliable.

Mr. SCHROCK. I agree. Mr. Chairman, just let me make one more comment. It is kind of ironic, but everybody that sits from that desk back, the minute we get sworn in we can get any briefing we want, no matter how good or bad we have been before we got here. So there is a fallacy in the thing right now. Maybe some of us should not have clearances.

Mr. LEONARD. Actually, the vetting process I think you went through, Congressman, is a whole lot more than we go through.

Mr. SCHROCK. Well, I was a career naval officer, so I went through that process. But there are a lot of people here that I look at and say, Hmm, should they have it. [Laughter.]

Chairman TOM DAVIS. I do not think we need to go there. [Laughter.]

Mr. SCHROCK. But that shows how out of whack this whole system is.

Chairman TOM DAVIS. Let me also just tail on. What if we codified the Executive order for reciprocity, would that help?

Mr. WILSHUSEN. That is certainly a valid option to try. One of the things that have not been able to quantify is the extent to which these reciprocity issues exist. But, certainly, that would be one option.

Chairman TOM DAVIS. We are going to hear on the next panel some issues. I am going to recognize Mr. Moran now, who is on the Defense Appropriations Committee, and that may be something that we would want to work on, Jim. We could get an authorization, you could put some language there that would help in some of these areas. I am going to recognize my friend from Virginia who has been very active on this issue as well. Mr. Moran.

Mr. MORAN. Thank you very much, Mr. Chairman. I know that you and apparently Ed as well, our district offices are inundated with these security issues. My district office director, and I have to believe it is exactly the same in your district office and probably with Ed's in the Tidewater area, said there are hundreds of people. And we are only taking the most egregious, the ones that do not make any sense. If there is any rationality to the process, we tell them you have just got to trust the system and at some point you are going to get the clearance. But we are only taking the egregious ones that do not make sense and we are overwhelmed with them. There is something wrong. Something has been wrong for quite a while here.

You have been giving us numbers and promises, and when I say us I am talking about the Congress. Chairman Davis is only holding this hearing because it has gone way past the point of any reasonable expectation of patience and deferring it to the executive branch. But DOD's performance standard, and there has been a lot of emphasis, sitting on Defense Appropriations, everybody that comes up talks about all the performance standards they are implementing and they are shaping everything up at DOD, and we have managers in there and we are going to do it right, and so on. So the DOD performance standard is 75 days for the initial secret clearance, 120 days for an initial top secret, and 180 days for reinvestigation of top secret. I wonder why it has to be 6 months for a reinvestigation. But the timeframe is now 375 days in fiscal year 2003, more twice than what the performance standard is. And this has been going on for years.

One of the problems is that there was an Executive order that was issued in 1995 that mandated that there be mutually and reciprocally accepted by all agencies. And yet, for some reason, this administration decided in April 2001 to disband that Executive order and to issue a brand new one. It was supposed to set up a different organization that was going to streamline this and it did just the opposite. And we now have a national security issue. We have a war going on and you are telling us to be patient—that is the word you used, Ms. Anderson—be patient, we are working it out, maybe next year we will transfer it over to OPM but we are still studying whether they can do the job or not. That is not acceptable. When you have almost 200,000 personnel that need to get to work serving this country and they cannot get their security clearance, it really is inexcusable. If you were on the other side of the aisle and you were looking at this, you would say somebody is not doing their job.

You have known this was the problem. As Chairman Davis has said, this was a report in 1981. But we have a war now, we have two wars going on and we cannot get the people we need out in the field. You come up here and tell us, well, we are working on it, be patient, we are studying it. The answer should be, "No excuses, sir." And what is most frustrating, you have never asked for any people. The Secretary never identified this, did not want anymore people provided to get the job done. Why? Why did you not ask for any people to get the job done? You know that we have an almost 200,000 backlog and you do not want any more people to do it. Do you want the backlog? Is there something we are missing here? Is there some explanation we are not figuring out, that you do not want these people cleared? Ms. Anderson, what?

Ms. ANDERSON. Sir, certainly, we want the people cleared. We will do nearly a million investigations this year. The request for additional personnel at Defense Security Service has been a longstanding debate within the Department of Defense. We believe that the decision to use more contractor resources will allow us the same degree of quality, better flexibility, and improved ability to increase the capacity.

Mr. MORAN. It sounds like I am reading something from a brochure, frankly. We believe that using more contractor personnel, why has it not happened? If you think that contract personnel are

going to fix it, then why did you not just fix it? If you are not asking for more people or Federal employees because you are going to contract it out, then why is it not contracted out? Why is it not getting done?

Ms. ANDERSON. DSS does have three contracts with contractor providers that have been immeasurably useful in helping reduce the numbers outstanding.

Mr. MORAN. Immeasurably useful.

Chairman TOM DAVIS. If the gentleman would yield?

Mr. MORAN. Yes, I would be happy to yield.

Chairman TOM DAVIS. GAO has identified this as a manpower problem to a great extent. So if you are not going to staff up because you are concerned about the ebb and flow, which you testified, and the highs and the lows, then over the short term you can contract this out. And it is unlimited. It would seem to me this is where, over a short term, you fire a contractor like that. But, clearly, you need more people for what is going on. And we do not have them. And what I am telling you, what Mr. Moran is telling you, and Mr. Schrock is telling you, we could get a lot of people in here to say let us get on with it. Let us not study it and get back by the end of the fiscal year, and then we can try maybe to hire somebody to put in a computer system. That is not going to cut it.

This backlog is huge and it is costing us more money everyday for people that we should not have to pay. You are taking money, my mother worked two jobs, she was a waitress at night and took care of other people's kids during the day, and you are taking money out of people like her's paycheck and overpaying, misspending it because you will not hire the people up front to do it. It is wrong. We want you to address it. This is serious.

Mr. MORAN. I could not have expressed it as well as you did, Mr. Chairman. Do you think for a moment that Defense Appropriations Committee, if you told us we need some staff or we need more money to contract out, you would not have gotten it? It is a $421 billion request. We will give you anything you need to get it done, and yet you do not want it. It is inexplicable and it is inexcusable. I do not know whether you are going to take this back to the Secretary, but somebody needs to write a note to the Secretary that we are going to present this stuff to the staff, and the Secretary is going to be pretty upset when he finds out that the Government Reform Committee had this hearing, Defense Appropriations wants to know what is going on, and he has never asked for anything from us to fix the situation. The situation is broken. The word is "broken." It is not working and you have to fix it. And it is going to take more than sweet talk and nodding. It has to be done now.

We have soldiers out in the field. They did not wait for a year. They were sent out there, some of them without adequate equipment, and we have contractors who could help them a whole heck of a lot with the technology we have available and they cannot go out because they have to wait more than a year for a security clearance. They have to go do other things. Most people that we really need are not going to wait around for a year till they get their security clearance. Thanks, Mr. Chairman.

Chairman TOM DAVIS. Thank you. Let me just make a comment. I remember the District of Columbia a few years ago was running

short on police. So to do their background checks, they just let everybody in and a couple of years later we had a huge scandal when a lot of these people who did not go through the clearances ended up stealing money and everything. So that is not the answer. The answer is we have to go through this. It does take some time. But we need personnel to do it. Get back to us, tell us what you need. And these decisions are made at a higher level. I do not mean to beat up on you. You drew the short straw today and you are here. [Laughter.]

We understand it and we appreciate your being here. And legislative action is coming. But this is costing us a lot of money and we are not as secure a country because of this, too. So, basically, the end result is we are getting less security and it is costing us more. So we need to address it.

And to OPM, this has to be given a high priority. This cannot be whenever. Everybody has a lot of priorities. We want to move this to the top of the stack because long term we cannot afford it.

Since 1981 it has been a problem. But now fighting a war on terror, it is very serious and the repercussions could be strong. And I do not want to get into what Ms. Watson got into about contracting and Iraq; I know where she was trying to go with this. Believe me, something goes wrong on this, it is going to come back to the clearances being backed up and everything else and there are serious ramifications. And from a cost-avoidance point of view, you ought to be up here at least asking for the money, and then if you do not get it, you are on record.

So thank you for being here. We appreciate it.

Mrs. Maloney, do you want to ask any questions? I will just yield to my friend from Virginia first, and then we will get to you, Mrs. Maloney.

Mr. MORAN. Just 30 seconds. D.C. is an excellent analogy. For years they went without hiring people, all kinds of bureaucracy, the few people there were overpaying them, they were sitting behind a desk. Reach a crisis situation and then we over-react and we dumped all these people without adequate training. And that could be what happens here. We are saying do the security clearances but figure out how to do them responsibly and expeditiously. Thank you, Mr. Chairman.

Chairman TOM DAVIS. The gentlelady from Manhattan, Mrs. Maloney.

Mrs. MALONEY. I thank the chairman for yielding. I would like to be associated really with the comments of Mr. Moran and Mr. Davis. It could not be stated more clearly. This is a scandal. You have to get on this and put the proper people, hire more people. Just get the job done.

I would like to raise one question of security clearance that deals specifically with Iraq. When I was there with the chairman on two oversight visits, some of the generals and top people really requested more people who spoke the language that they could trust. They felt they sometimes were, and there were even allegations of spies in some of their units and so forth, relying on people they did not really know to be interpreters. Maybe it has gotten better. But very few people really spoke the language. We have two, State Department and DOD, schools. I want to know how many people are

we training to speak the language? And are we getting people over there? That was a specific request to our delegation, to get more people over there who spoke the language who they would trust to interpret appropriately and would trust with inside information on where they are moving their vehicles and so forth. So, specifically, security clearance and training for language-speaking officials for Iraq and Afghanistan, where does that stand?

Ms. ANDERSON. Ma'am, we understand the importance of having trusted, vetted individuals in country to serve as the linguists. I know that the Defense Intelligence Agency has put the vetting of those individuals at the top of their list. We know that the services and agencies are recruiting people within their own ranks. I do not have specific numbers with me, but we are happy to get those over here.

Mrs. MALONEY. But my question—they said they are trying to vet as best as they can, but it was a real weakness in our operation over there and that they needed more people speaking the language. And they requested us to go back and get more people trained out of America or in Qatar or some place that they could get over there. And I just wonder, are our language schools focusing on that? How many people are we training in the language now? They obviously are going to have security clearance coming from our country. So if you could get back to us maybe on how we are training in our country or in Qatar or wherever to get people over there that they can trust and they can work with. Thank you.

Chairman TOM DAVIS. Thank you. Anyone want to add anything at this point? You want to get out of here, don't you? [Laughter.]

Thank you all for being with us.

We will take about a 2-minute recess as we get our next panel ready.

For our second panel we have a very distinguished panel. We have Sudhakar V. Shenoy, chairman of the Northern Virginia Technology Council, a graduate of the Indian Institute of Technology. We have Bobbie Kilberg, president of the Northern Virginia Technology Council. And Bobbie, I understand that Gary Nakamoto is going to be sworn in as well. If we have any tough questions, we can go to Gary, our go-to guy. And also with us is Douglas Wagoner, the chairman of the Intelligence and Security Task Group of the Information Technology Association of America. You all have heard the previous testimony. I almost wish that I could have put you first so that they could, instead of no problem, we are working on it, they could understand the seriousness of this. I know Mr. Moran is going to be back, Members are going to be back. We may have a vote in between, but I want to get the testimony here on the record as quickly as we can. So I need to swear you in. Mr. Nakamoto, you are there as well.

[Witnesses sworn.]

Chairman TOM DAVIS. I think you know the rules on the lights.

Mr. Shenoy, we will start with you. Thank you very much for being here and for coming forward. I know you are speaking for a lot of businesses, not just in Northern Virginia but all across the country, that are experiencing these difficulties.

STATEMENTS OF SUDHAKAR V. SHENOY, CHAIRMAN, NORTHERN VIRGINIA TECHNOLOGY COUNCIL; BOBBIE G. KILBERG, PRESIDENT, NORTHERN VIRGINIA TECHNOLOGY COUNCIL, ACCOMPANIED BY GARY NAKAMOTO, NVTC; AND DOUGLAS WAGONER, CHAIRMAN, INTELLIGENCE AND SECURITY TASK GROUP, INFORMATION TECHNOLOGY ASSOCIATION OF AMERICA

Mr. SHENOY. Thank you, Mr. Chairman. Good morning, Mr. Chairman and committee members. The Northern Virginia Technology Council wants to personally thank you for holding this hearing and for your leadership on national security and the issues raised by the Federal Government's present security clearance process.

I appear before you this morning as chairman of the Northern Virginia Technology Council [NVTC], and also as chairman and CEO of Information Management Consultants, Inc., a northern Virginia based company. I am accompanied by Bobbie Kilberg, who is the president of NVTC. The Northern Virginia Technology Council is the membership and trade association for the technology community in northern Virginia and is the largest technology council in the Nation, with over 1,200 member companies representing about 160,000 employees.

From the late 1990's through 2001, the northern Virginia region saw an incredible boom in business driven largely by investment in technology. Our community saw enormous expansion of existing companies and the creation of hundreds of new entities. Our work force needs exceeded the supply of available workers and unemployment rates dipped as low as 1.5 percent. NVTC's work force initiatives sought to attract talented and qualified workers to the region through various incentives and programs.

Since the tragic events of September 11, northern Virginia, like many other high-tech regions, experienced downturns in investment and significant lay-offs of employees. Fortunately for the region, many of the businesses have been able to retool and innovate in areas that can be of assistance to the national security efforts of the United States. Our companies have been able to develop new technologies for use in the defense of our country and have been able to pull out of a recessionary climate through participation in Federal Government contracts. Herein lies the work force dilemma.

After thorough consultation with NVTC's technology company members, the NVTC Workforce Committee has determined that the major causes for the delays in the security clearance process are as follows: Lack of resources at the agency level to timely process applications; unnecessary increases in the level and number of security clearances involved in many contracts; inability to move a secured worker from one agency contract to the contract of another agency without going through another separate clearance process; disparate adjudication methods at the agencies; antiquated methods of conducting background checks; and lack of technology-based processing of contractor security clearances.

The inability of NVTC member companies, which are Federal Government contractors or wish to enter that market, to obtain security clearances in a timely and efficient manner has the following ramifications: Inability of companies to enter the Government con-

tracting arena because of the lack of a cleared work force; inability of companies who are Government contractors to fill many open positions by hiring highly skilled workers, who have been laid off in the region and who would qualify for these open positions, because of the excessive length of time required to obtain security clearances. Companies cannot afford to keep skilled workers "on the bench" while awaiting the completion of a security clearance; competition for workers with security clearances is intense with Government contractors hiring away each others' employees at ever increasing wages; cleared workers are recruited away from the military and other Government agencies where they are performing important functions; and increased costs to companies for hiring cleared workers translate into increased costs presented in contract bids to Government agencies.

In December 2003, NVTC conducted a security clearance survey of its membership to formalize the anecdotal evidence we had compiled. We developed a 15 question electronic survey which we sent to 703 of our member companies, receiving an overall response rate of 22.5 percent. We found that more than one half of the respondent companies had over 50 percent of their business in Government contracting. We also found that small businesses were highly represented in the survey sample. In response to questions about the number of unfilled positions due to inability to find cleared workers, 73 percent of the responders reported open positions in secret, top secret, and sci/poly clearance categories. In response to questions about the ability of companies to find cleared employees, the majority of respondents indicated that it was either "somewhat difficult" or "very difficult" to find cleared workers. When asked about hiring methods for finding new employees with clearances, nearly 70 percent of the respondents reported that they recruit directly from the Government or other Federal contractors. In addition, more than half of the respondents said they paid a minimum 10 percent premium to recruit cleared workers for their companies. If a security clearance application was submitted, 50 percent of the respondents were required to wait 6 months or longer for a response. For the top secret and sci/poly clearances, our members indicated a 12 to 18 month wait period.

It is of critical importance that this committee require reform of the Nation's security clearance system and we recommend that the following reforms be instituted through administrative and/or legislative action: 1Reciprocity among agencies—codification of Executive Order 12968; portability between agencies—again, codification of Executive Order 12968; re-evaluation of clearance requirements to be certain they are necessary; provision for self-initiated preprocessing of security clearance with a Letter of Intent to hire; reexamination of funding sources to pay costs for clearances; re-examination of the factors for disqualification; and investment in and better use of technology to conduct efficient, secure, and consistent background checks.

NVTC and its member companies are willing to assist in any way that is helpful to the committee, and we thank you for inviting us to testify before you today. Thank you.

[The prepared statement of Mr. Shenoy follows:]

Testimony of Sudhaker V. Shenoy
Chairman of the Northern Virginia Technology Council

Before
U.S. House of Representatives
Committee on Government Reform
Security Clearance Backlogs and Reciprocity Issues for Defense Industry Personnel
May 6, 2004

Good Morning Mr. Chairman and committee members. The Northern Virginia Technology Council wants to personally thank you for holding this hearing and for your leadership on national security and the issues raised by the federal government's present security clearance process.

I appear before you this morning as Chairman of the Northern Virginia Technology Council (NVTC) and also as Chairman and the CEO of Information Management Consultants, Inc. I am accompanied by Bobbie Kilberg, President of NVTC.

NVTC Background

The Northern Virginia Technology Council ("NVTC") is the membership and trade association for the technology community in Northern Virginia and is the largest technology council in the nation with over 1,200 member companies representing about 160,000 employees. Our membership includes companies from all sectors of the technology industry including information technology, software, Internet, ISPs,

telecommunications, biotechnology, bioinformatics, aerospace and nanotechnology, as well as the service providers that support these companies.

Workforce Committee of NVTC

The charter of the NVTC Workforce Committee is to assist member companies with the recruitment, education, and retention of a world class workforce that is capable of creatively solving complex technology challenges and inspiring the entrepreneurial spirit of employees and organizations. This mission has been challenged by the serious issues that our technology companies encounter as their need for workers with security clearances for federal contracts rapidly increases but their ability to obtain these clearances is seriously hampered both by unnecessary procedural hurdles and excessive processing time. The problems surrounding security clearance issues have become such a major concern to our members that, for the last three years, the primary advocacy mission of the NVTC Workforce Committee has been to address this issue, under the able leadership of Laura Reiff from Greenberg Traurig, Karla Leavelle from George Mason University, and Michael Ferraro from Training Solutions, Inc.

The Security Clearance Issue

From the late 1990s through 2001, the Northern Virginia region saw an incredible boom in business driven largely by investment in technology. Our community saw enormous expansion of existing companies and the creation of hundreds of new entities. Our

workforce needs exceeded the supply of available workers and unemployment rates dipped as low as 1.5%. NVTC's workforce initiatives sought to attract talented and qualified workers to the region through various incentives and programs.

Since the tragic events of September 11, Northern Virginia, like many other high-tech regions, experienced downturns in investment and significant lay-offs of employees. Fortunately for the region, many of the businesses have been able to re-tool and innovate in ways that can be of assistance to the national security efforts of the U.S. Our companies have been able to develop new technologies for use in the defense of our country and have been able to pull out of a recessionary climate through participation in federal government contracts. Herein lies the workforce dilemma.

While NVTC member companies are working in conjunction with the federal government on important contracts, the demand to maintain and increase the security clearances for their employees has risen. Our members have seen an increase in the level of security clearances that are required on many existing contracts. We also have seen an increase in the clearance requirements for new contracts. These increases, coupled with significant processing delays to obtain clearances at all levels, has highlighted this issue as a major workforce problem.

After thorough consultation with NVTC's technology company members, the NVTC Workforce Committee has determined that the major causes for the delays in the security clearance process are as follows:

- Lack of resources at the agency level to timely process applications;
- Unnecessary increases in the level and number of security clearances involved in many contracts;
- Inability to move a secured worker from one agency contract to the contract of another agency without going through another separate clearance process;
- Disparate adjudication methods at the agencies;
- Antiquated methods of conducting background checks; and
- Lack of technology-based processing of contractor security clearances.

The inability of NVTC member companies, which are federal government contractors or wish to enter that market, to obtain security clearances in a timely and efficient manner has the following ramifications:

- Inability of companies to enter the government contracting arena because of the lack of a cleared workforce;
- Inability of companies who are government contractors to fill many open positions by hiring highly skilled workers, who have been laid off in the region and who would qualify for these open positions, because of the excessive length of time required to obtain security clearances. Companies cannot afford to keep skilled workers "on the bench" while awaiting the completion of a security clearance;
- Competition for workers with security clearances is intense with government contractors hiring away each others' employees at ever increasing wages;

- Cleared workers are recruited away from the military and other government agencies where they are performing important functions; and
- Increased costs to companies for hiring cleared workers translate into increased costs presented in contract bids to government agencies.

These issues are particularly troublesome for our smaller member companies as they have more significant hurdles to entry into the government contracting market.

In December 2003, NVTC conducted a security clearance survey of its membership to formalize the anecdotal evidence we had compiled. The survey was conducted by Lynne Kaye of the Hay Group, which donated her time to this project. The survey is attached to this testimony and is submitted as part of the record. We developed a 15 question electronic survey which we sent to 703 of our member companies, receiving an overall response rate of 22.5%. We found that more than one half of the respondent companies had over 50% of their business in government contracting. We also found that small businesses were highly represented in the survey sample. In response to questions about the number of unfilled positions due to inability to find cleared workers, 73% of the respondents reported open positions in secret, top secret and sci/poly clearance categories. In response to questions about the ability of companies to find cleared employees, the majority of respondents indicated that it was either "somewhat difficult" or "very difficult" to find cleared workers. When asked about hiring methods for finding new employees with clearances, nearly 70% of respondents reported that they recruit directly from the government or other federal contractors. In addition, more than half of

the respondents said they paid a minimum 10% premium to recruit cleared workers to their companies. If a security clearance application was submitted, 50% of the respondents were required to wait six months or longer for a response. For the top secret and sci/poly clearances, our members indicated 12-18 month waiting periods.

Much of our testimony has highlighted the problems and costs of the growing security clearance backlog. However, it is equally important to bring to the Committee's attention some technological solutions that are currently in development by NVTC member companies through research and development funding from the intelligence community. We think that double the number of clearances can be processed in the same amount of time, by the same number of staff, with no compromise in quality, utilizing a combination of technology and innovative streamlining techniques. Results can and should be easily shared across different agencies.

Our member companies have worked directly with some of the federal government's best investigators. Companies are now encoding the entire investigative process into a web-based tool. They are automating the report writing process, reducing the amount of time agents spend documenting their results by 50% or more. In addition, the results of each investigation will be more comprehensive, consistent and streamlined. Funding for developing full scale solutions must be continued in order to allow these types of technologies to be deployed through the government.

It is of critical importance that this Committee require reform of the nation's security clearance system and we recommend that the following reforms be instituted through administrative and/or legislative action:

- Reciprocity among agencies – codification of Executive Order 12968;
- Portability between agencies – codification of Executive Order 12968;
- Re-evaluation of clearance requirements to be certain they are necessary;
- Provision for self-initiated, pre-processing of security clearances with a Letter of Intent to hire;
- Re-examination of funding sources to pay for costs of clearances;
- Re-examination of the factors for disqualifications; and
- Investment in and better use of technology to conduct efficient, secure and consistent background checks.

NVTC and its member companies are willing to assist in any way that is helpful to the Committee and we thank you for inviting us to testify before you today.

NVTC
NORTHERN VIRGINIA TECHNOLOGY COUNCIL

March 19, 2003

BOARD OF DIRECTORS
Sudhakar Shenoy, Information Management Consultants
Chairman
Bobbie Kilberg, Northern Virginia Technology Council
President
John Lee, IV, Lee Technologies Group
Vice-Chairman
Dendy Young, GTSI
Vice-Chairman
Steve Tolbert, Global Systems & Strategies Inc.
Secretary
Tony Buzzelli, Deloitte & Touche
Treasurer
J. Scott Hommer III, Venable, Baetjer & Howard, LLP
General Counsel
Doug Perritt, Qorvis Communications
Public Relations Advisor

Panos Anastassiadis, Cyveillance
Paul Broome, ENSCO
John Burton, Updata Capital
Craig Chason, Shaw Pittman
Anne Crossman, Completed Systems, Inc.
Caren DeWitt, webMethods Foundation
Al Edmonds, EDS Corporation
C. Michael Ferraro, TRAINING SOLUTIONS, Inc.
Kevin Fitzgerald, Oracle
Dev Ganesan, TRADOS
Daniel Gonzales, USI Real Estate
Neal Grunstra, Mindbank
Deepak Hathiramani, Vatronix, Inc.
Tom Hicks, Wilmer, Cutler & Pickering
Steven Hoffman, Blackboard, Inc.
L. Kenneth Johnson, CACI
Bob Kahn, Corp. for National Research Initiatives
Jim LeBlanc, Global Smarts, Inc.
Paul Lombardi, DynCorp
Lisa Martin, LeapFrog Solutions
Duffy Mazao, SolutionWorx
Gary McCollum, Cox Communications
Tiff McNeill, TranTech
Linda Mills, Northrop Grumman
Donna Morea, AMS
Ray Ogilthorpe, America Online, Inc.
Gary Pan, Panacea Consulting
Leslie Plott, Foundation for Genetic Medicine
Todd Rowley, First Union/Wachovia
Chris Schroeder, TechNews.com
Jonathan Shanes, Ernst & Young
Tim Tong, George Washington University
Erich Windmuller, IBM

CHAIRMAN EMERITUS
John Backus, Draper Atlantic
Daniel Bennister, DynCorp
Edward H. Bersoff, Quarterdeck Investment Partners
Kathy Clark
Michael A. Daniels, SAIC
David C. Laciea, CMS Information Services

HONORARY MEMBERS
Michael J. Lewis, Am. Inst. of Aeronautics & Astronautics

SENIOR ADVISORY
Marie Morino, Morino Institute
Philip Odeen, TRW
Lee Pesatis, webMethods Federal
Wayne Shelton
J. Knox Singleton, InovaHealth Systems
Esther T. Smith, Qorvis Communication
Bob Templin, Northern Virginia Community College
John Toups
Earle Williams
Robert L. Wright, Dimensions International, Inc.

Dear Senator:

As Chairman and President of the Northern Virginia Technology Council ("NVTC"), we are writing to urge you to reform the nation's security clearance system so it will better serve both our national security and economic security needs. At present, the system is unnecessarily complex and inefficient, slow and duplicative among federal departments and agencies.

NVTC is the membership association for the technology community in Northern Virginia with approximately 1,500 member companies representing over 170,000 employees. Our membership includes companies from all sectors of the technology industry including information technology, software, Internet, ISPs, ASPs, telecommunications, biotech, and aerospace, as well as the service providers that support these companies. NVTC is the largest technology council in the United States and has become the voice of technology for our region.

National security is of critical importance to our member businesses. Many NVTC member companies were directly affected by the 9/11 terrorist strikes and, both as citizens and as business leaders, we want to help prevent future attacks. In this spirit, we note that there are technology workers throughout the country who are ready and willing to assist our government in the process. The only major hurdle for this human capital is the security clearance process.

The federal government's security clearance procedures are not efficient, specifically for those who are not currently government employees. The length of time to process these clearances is growing and the cost of the process, including the opportunity cost of delayed projects and overhead, is staggering. There are disparate adjudication methods used by the various departments and agencies. These and many other substantive and procedural clearance "requirements" have led to a security clearance crisis. Cannibalism between the federal government and defense contractors for cleared workers is routine. This leads to higher costs to the government in addition to the inability to adequately staff projects with cleared personnel.

The following are recommendations for substantive and procedural changes in the present security clearance system:

- Reciprocity and portability among departments and agencies
- Self initiated, pre-processing with a Letter of Intent to hire
- Re-examination of funding sources to pay for costs of clearances (DOL initiatives)
- Re-examination of factors for disqualifications
- Re-examination of length of clearance and renewal procedures
- Better use of technology to improve, streamline and shorten the clearance process
- Reevaluation of the need for some positions to have a clearance

Please note that reform of the security clearance process was one of the recommendations of a NVTC working group report to the Panel on Terrorism of the President's Council of Advisors on Science and Technology.

On behalf of the Northern Virginia Technology Council, we urge you to reform the federal security clearance system to meet our present and future challenges. There is broad support for this type of reform and we would like to work with you on this task.

Sincerely,

Sudhakar Shenoy
Chairman
The Northern Virginia Technology Council

Bobbie Kilberg
President
Northern Virginia Technology Council

NVTC

NORTHERN VIRGINIA TECHNOLOGY COUNCIL

March 19, 2003

BOARD OF DIRECTORS
Sudhakar Shenoy, Information Management Consultants
Chairman
Bobbie Kilberg, Northern Virginia Technology Council
President
John Lee, IV, Lee Technologies Group
Vice-Chairman
Dendy Young, GTSI
Vice-Chairman
Steve Tolbert, Global Systems & Strategies Inc.
Secretary
Tony Buzzelli, Deloitte & Touche
Treasurer
J. Scott Hommer III, Venable, Baetjer & Howard, LLP
General Counsel
Doug Perets, Qorvis Communications
Public Relations Advisor

Panos Anastassiadis, Cyveillance
Paul Broome, ENSCO
John Burton, Updata Capital
Craig Chason, Shaw Pittman
Anne Crossman, Completed Systems, Inc.
Caren DeWitt, webMethods Foundation
Al Edmonds, EDS Corporation
C. Michael Ferraro, TRAINING SOLUTIONS, Inc.
Kevin Fitzgerald, Oracle
Dev Ganesan, TRADOS
Daniel Gonzales, USI Real Estate
Neal Grunstra, Mindbank
Deepak Hathiramani, Vistronix, Inc.
Tom Hicks, Wilmer, Cutler & Pickering
Steven Hoffman, Blackboard, Inc.
L. Kenneth Johnson, CACI
Bob Kahn, Corp. for National Research Initiatives
Jim LeBlanc, Global Smarts, Inc.
Paul Lombardi, DynCorp
Lisa Martin, LeapFrog Solutions
Duffy Matau, SolutionWorx
Gary McCollam, Cox Communications
TiTi McNeill, TranTech
Linda Mills, Northrop Grumman
Donna Morea, AMS
Ray Ogilthorpe, America Online, Inc.
Gary Pan, Parsons Consulting
Leslie Platt, Foundation for Genetic Medicine
Todd Rowley, First Union/Wachovia
Chris Schroeder, TechNews.com
Jonathan Shames, Ernst & Young
Tim Tong, George Washington University
Erich Wiedmuller, IBM

CHAIRMAN EMERITUS
John Backus, Draper Atlantic
Daniel Bannister, DynCorp
Edward H. Bersoff, Quarterdeck Investment Partners
Kathy Clark
Michael A. Daniels, SAIC
David C. Lucius, CMS Information Services

HONORARY MEMBERS
Michael J. Lewis, Am. Inst. of Aeronautics & Astronautics

SENIOR ADVISORY
Mario Morino, Morino Institute
Philip Odeen, TRW
Lee Pometa, webMethods Federal
Wayne Shelton
J. Knox Singleton, InovaHealth Systems
Esther T. Smith, Qorvis Communications
Bob Templin, Northern Virginia Community College
John Toups
Earle Williams
Robert L. Wright, Dimensions International, Inc.

Dear Representative:

As Chairman and President of the Northern Virginia Technology Council ("NVTC"), we are writing to urge you to reform the nation's security clearance system so it will better serve both our national security and economic security needs. At present, the system is unnecessarily complex and inefficient, slow and duplicative among federal departments and agencies.

NVTC is the membership association for the technology community in Northern Virginia with approximately 1,500 member companies representing over 170,000 employees. Our membership includes companies from all sectors of the technology industry including information technology, software, Internet, ISPs, ASPs, telecommunications, biotech, and aerospace, as well as the service providers that support these companies. NVTC is the largest technology council in the United States and has become the voice of technology for our region.

National security is of critical importance to our member businesses. Many NVTC member companies were directly affected by the 9/11 terrorist strikes and, both as citizens and as business leaders, we want to help prevent future attacks. In this spirit, we note that there are technology workers throughout the country who are ready and willing to assist our government in the process. The only major hurdle for this human capital is the security clearance process.

The federal government's security clearance procedures are not efficient, specifically for those who are not currently government employees. The length of time to process these clearances is growing and the cost of the process, including the opportunity cost of delayed projects and overhead, is staggering. There are disparate adjudication methods used by the various departments and agencies. These and many other substantive and procedural clearance "requirements" have led to a security clearance crisis. Cannibalism between the federal government and defense contractors for cleared workers is routine. This leads to higher costs to the government in addition to the inability to adequately staff projects with cleared personnel.

The following are recommendations for substantive and procedural changes in the present security clearance system:

- Reciprocity and portability among departments and agencies
- Self initiated, pre-processing with a Letter of Intent to hire
- Re-examination of funding sources to pay for costs of clearances (DOL initiatives)
- Re-examination of factors for disqualifications
- Re-examination of length of clearance and renewal procedures
- Better use of technology to improve, streamline and shorten the clearance process
- Reevaluation of the need for some positions to have a clearance

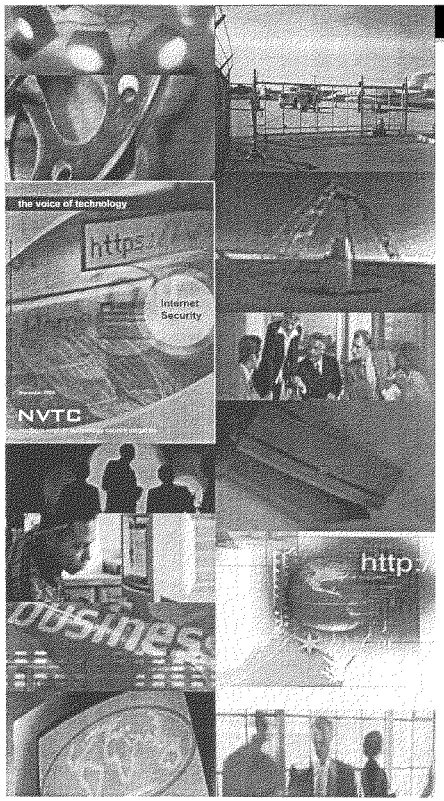
Please note that reform of the security clearance process was one of the recommendations of a NVTC working group report to the Panel on Terrorism of the President's Council of Advisors on Science and Technology.

On behalf of the Northern Virginia Technology Council, we urge you to reform the federal security clearance system to meet our present and future challenges. There is broad support for this type of reform and we would like to work with you on this task.

Sincerely,

Sudhakar Shenoy
Chairman
The Northern Virginia Technology Council

Bobbie Kilberg
President
Northern Virginia Technology Council



NVTC Security Clearance Survey Results

December, 2003

Our special thanks to the Hay Group for organizing this survey.

Hay Group
4301 N. Fairfax Drive, Suite 500
Arlington, VA 22203
(703) 841-3100 (phone)
(703) 908-3000 (fax)

Executive Overview

Executive Overview
- What is Northern Virginia Technology Council
- Introduction
- The Survey
- Summary of Survey Findings

Review of All Survey Findings
- Survey Response Rate
- Survey Respondent Demographics
- Backlog of Secured Positions
- Time to Receive Clearances
- Difficulty of Receiving Clearances
- Pay and Hiring Practices
- Strategies for Managing Shortage
- Improving Clearance Process



What Is Northern Virginia Technology Council (NVTC)?

- A membership association for the technology community in Northern Virginia
- The largest technology council in the United States
- Founded in 1991
- Representing more than 1300 member companies, equally divided between technology member companies and associate members
- Our membership includes information technology, software, Internet, ISPs, telecommunications, biotechnology, bioinformatics, aerospace and nanotechnology, as well as the service providers that support these companies
- Representing more than 170,000 employees



Introduction

Many NVTC member companies were directly affected by the 9/11 terrorist strikes and, both as citizens and as business leaders, we want to help prevent future attacks. In this spirit, we note that there are technology workers throughout the country who are ready and willing to assist our government in the process. The only major hurdle for this human capital is the security clearance process.

The business results of these conditions are:

- The length of time to process these clearances is growing and the cost of the process, including the opportunity cost of delayed projects and overhead, is staggering.



Introduction (continued)

- There are disparate adjudication methods used by the various departments and agencies.
- There are higher costs to the government in addition to the inability to adequately staff projects with cleared personnel.
- Some contractors do not have enough cleared staff members to compete for contracts for which they have the technical qualifications and relevant experience
- Contractors hire cleared workers from one another and the federal government which drives up pay for cleared workers and increases the government's cost
- Employers cannot afford to tap into the existing pool of unemployed, skilled workers because they cannot get the workers cleared and billable fast enough
- Some firms exited the Federal sector or elected to focus exclusively on contracts that do not require clearances



The Survey

At the request of the House Committee on Government Reform, NVTC decided to survey its members to obtain statistical data on the security clearance situation.

- NVTC developed a 15 question survey, including two open ended questions; and
- Administered the survey online to all NVTC technology members and a few associate members identified as government contractors.
- Total number of survey invitation emails sent = 703



Summary of Survey Findings

- Overall response rate 22.5%
- The number of government contractors responding to the survey represents 30% of NVTC's technology members who are identified government contractors
- More than half of the respondents have 50 or fewer employers, which mirrors the NVTC technology membership



Summary of Survey Findings

Secret Clearance

73% report having one to more than 500 positions open requiring a Secret

59% report it takes 6 months or longer to acquire a Secret

Top Secret Clearance

63% report having one to more than 500 positions open requiring a Top Secret

94% report it takes 6 months or longer to acquire a Top Secret

70% report it takes 12 months or longer to acquire a Top Secret

SCI/Poly Clearance

57% report having one to more than 500 positions open requiring a SCI/Poly

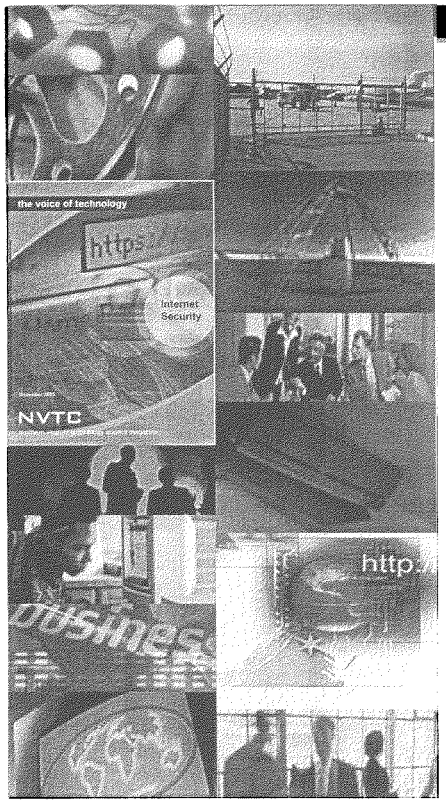
90% report it takes 12 months or longer to acquire a SCI/Poly



Summary of Survey Findings

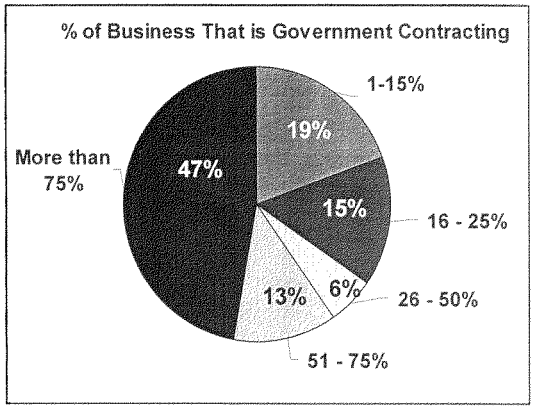
- More than 50% of respondents indicted that it is "somewhat difficult"or "very difficult" to fill job openings that require each of the three categories of clearance.
- Nearly 70% of the respondents indicated they fill job openings by recruiting cleared workers from other government contractors or the government
- More than half of the respondents pay a minimum 10% premium to cleared workers and many pay more than a 25% premium



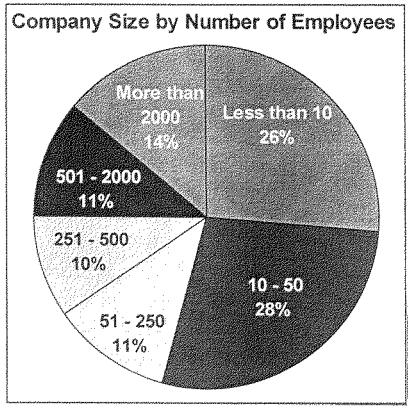


Review of All Survey Findings

Survey Respondent Demographics



More than one-half of respondents' companies have over 50% of their business in government contracting.

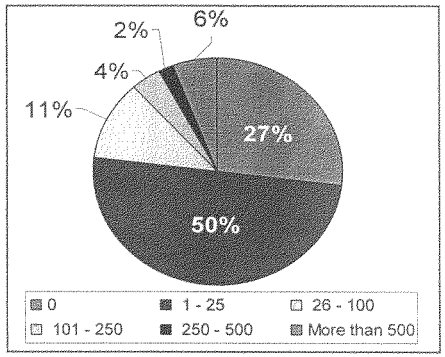


Small business is highly represented in survey sample, which mirrors NVTC membership



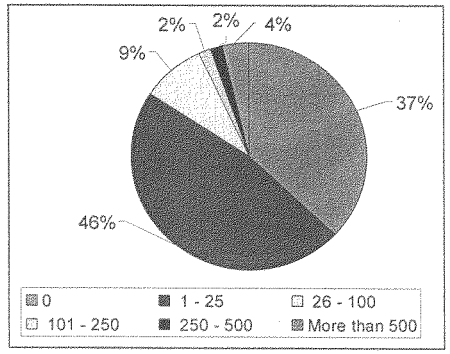
Backlog of Secured Positions

Number of unfilled positions - Secret



73% have one to more than 500 open positions requiring a Secret

Number of unfilled positions - Top Secret

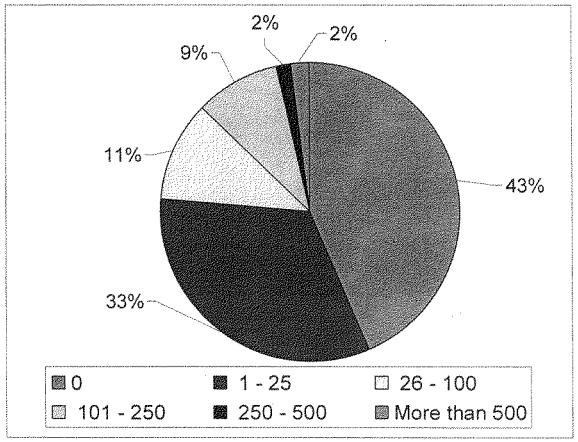


63% have one to more than 500 open positions requiring a Top Secret



Backlog of Secured Positions

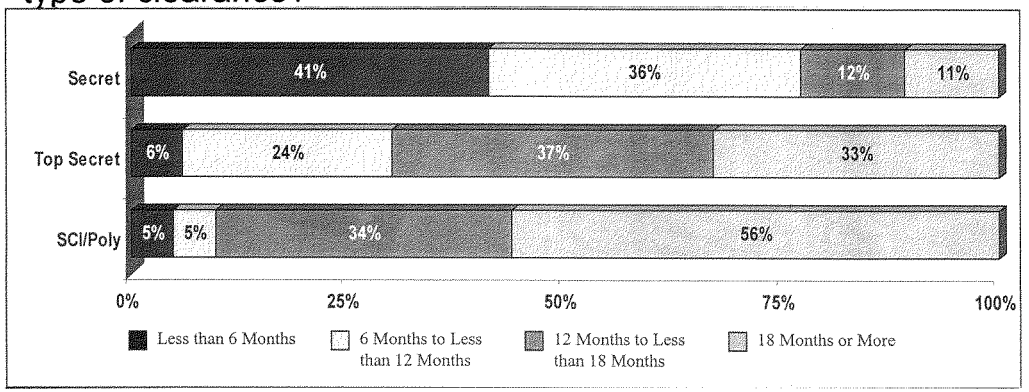
Number of unfilled positions - SCI/Poly



57% have one to more than 500 open positions requiring a SCI/Poly

Time to Receive Clearances

In your experience, how long does it generally take for each type of clearance?

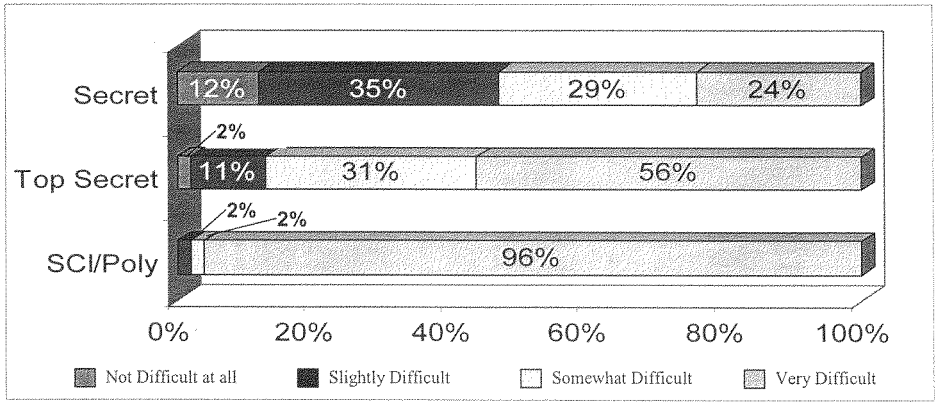


In all categories more than 50% of respondents wait 6 months or longer for a cleared worker



Difficulty of Receiving Clearances

How difficult is it to find cleared employees to fill job openings that require each type of clearance?

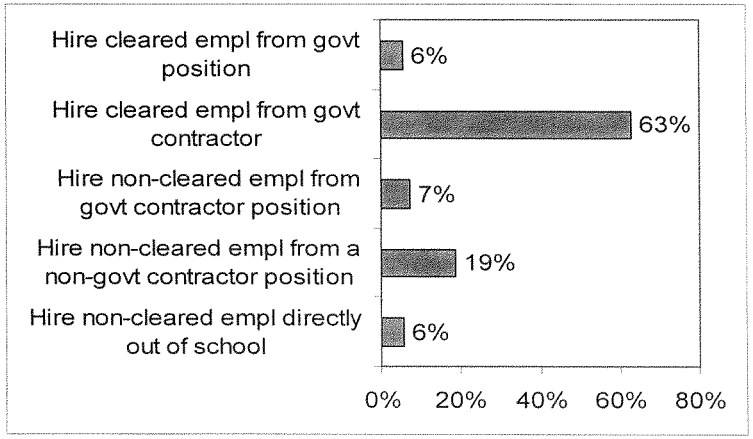


Majority of respondents indicate that it is "somewhat difficult" or very difficult" to find cleared workers



Hiring Practices

How do you typically hire new employees who require a clearance?

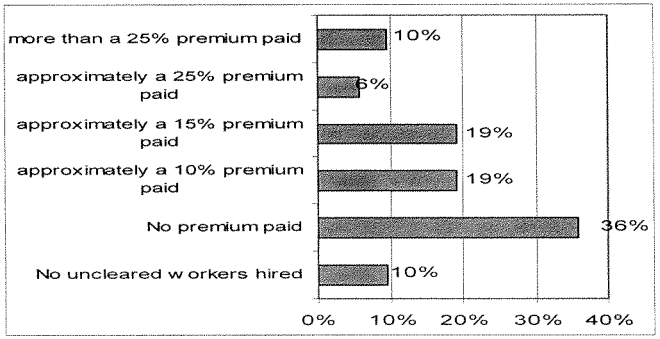


Nearly 70% of respondents recruit only cleared workers from government or other contractors.



Pay Practices

On average, how much of a premium do you pay to have a cleared worker as opposed to an uncleared worker?



More than half of the respondents pay a minimum 10% premium to cleared workers



Strategies for Managing Shortage

Recruiting

- Offer special projects with interesting content
- Offer signing bonuses to cleared workers
- Provide monetary incentives to existing employees that recruit cleared workers
- Target government workers close to retirement
- Target those exiting the military

(key themes in response to the open ended questions)



Strategies for Managing Shortage

Clearance Process

- "Warehouse" candidates for TS/SCI projects on uncleared or lower cleared projects while awaiting TS/SCI
- Clear internal workers in advance and cross-train them to work on projects requiring clearances
- Establish a special team within the company that has specialized expertise in the clearance process

(key themes in response to the open ended questions)

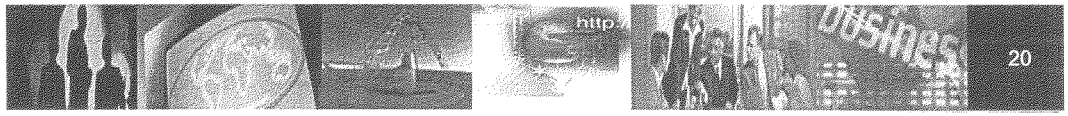


Strategies for Managing Shortage

Contract Structure

- Use cleared management to divide work into cleared and uncleared portions to reduce level of effort of cleared people
- Negotiate with customer to allow uncleared or lower cleared people to perform with a cleared escort

(key themes in response to the open ended questions)



Suggestions for Improving the Clearance Process

- Divide tasks within contract by clearance level. For example, development work could be done on an uncleared basis while populating the data would require a clearance
- Educate Federal employees writing contracts on the financial and time impact of requiring higher clearances for tasks that could be performed with lower clearances or on an uncleared basis
- Redesign clearance process so that multiple steps could occur in parallel such as administering the polygraph while the background check is taking place

(key themes in response to the open ended questions)



Suggestions for Improving the Clearance Process

- Reciprocity and portability among departments and agencies
- Create a central database of basic information so that individuals do not have to complete the same form in its entirety each time they apply for a clearance
- Agencies should inform the contractor when a clearance or clearance transfer is complete rather than asking the contractor to keep visiting the Agency's website to see whether the clearance is posted

(key themes in response to the open ended questions)



Chairman TOM DAVIS. Thank you very much.

Ms. Kilberg.

Ms. KILBERG. I took some notes based on the testimony before from the Government and I would love to spend a few minutes just making some comments.

Chairman TOM DAVIS. OK. I would love to hear you.

Ms. KILBERG. OK. No. 1, one of the things we have not focused on but we should is that much of the innovation and cutting-edge technology to fight terrorism comes from small- and mid-sized companies. The security clearance debacle means that it is simply not competitive for most of those companies to be able to get those contracts. They shy away from competing because with the security clearance problem they cannot succeed. That is not good for innovative solutions and we really need to look at that.

Second, I want to take a few minutes to go through our member company survey just to give you a real indepth feel. For secret level clearances, our companies report that more than 6 months is required from our member companies' perspectives. Fifty-nine percent said it takes more than 6 months to get those clearances. Top clearance level, 70 percent say it takes 12 to 18 months, and 33 percent said it takes 18 months or longer. Sci/poly clearance level, 90 percent said it takes more than 12 months, and 56 percent said it takes 18 months or longer.

Third, I think I heard the gentleman from OPM saying that they now have a RFP out for contractors. I think that is a way, an approach to deal with this issue. However, the investigators that the contractors are going to use themselves have to be cleared themselves. And if I heard him correctly, in the RFP the contractor applying cannot raid or recruit people from the Government or other contractors. So if they cannot themselves get people who are already cleared to be the investigators to do the clearances, you are just going to get yourself more and more in a catch–22.

Next point, DOD. Twenty-five months for reform. As Congressman Schrock said, that is just frightening. That is truly, truly scary.

Next point, and I was not going to bring it up but Congressman Moran mentioned it, what do our companies do in this region when they have people problems? They go to their Congressmen. They go to all of you and they put insistent pressure and say help us, help us, we cannot get cleared. That is not the way the system should work. But that is their only way to get clearances in a timely manner now, and that is going on throughout the country.

Codifying Executive orders. That is very important. But, as Congressman Davis said, if that is not accompanied by additional Federal money, we are only codifying something on paper and nothing is going to change.

Two final points. I do not mean to be pejorative, but obviously, as Congressman Davis said, Heather Anderson drew the short straw and that is why she is here today. And I worry about how long it is going to take her to get through the Department of Defense bureaucracy to let Secretary Rumsfeld know what happened today at this hearing. And if it takes her 6 months to do that, you are another 6 months behind.

And finally, we need to use technology to help solve this problem and we are not presently using it as effectively as we can. One very quick example. One of the things that was not discussed but is obviously important is re-clearances, a person has a clearance and then they have to be re-cleared. One of the things that the White Paper which ITAA, NVTC and all of us in the coalition developed, discusses is the fact that, if you could develop a standard structure for security clearance requirements, then you could facilitate a system to monitor the continuing validity of clearances. And given the technology you have today in data mining, you could have an ongoing data base that would be able to tell you immediately whether there is a change in status—an arrest, a bankruptcy, an unexplained affluence—things that might indicate a potential security risk even before you normally would do that re-clearance or that reevaluation. If you could do that and you could identify potential security issues quickly and efficiently through technology, then you could reduce reinvestigation time and you could free up resources to focus on new clearances.

Those are just some points from my notes and from listening this morning. Thank you.

Chairman TOM DAVIS. Thank you very much. My instinct is that Secretary Rumsfeld probably has other things on his mind today than just worrying about expediting security clearances. But we can get this word to the appropriate people in Defense that can take action, it does not have to start at that level, and we intend to do that. So I appreciate your remarks.

Mr. Wagoner, thank you for being with us.

Mr. WAGONER. Mr. Chairman and members of the committee, thank you for inviting ITAA to testify today on the challenges industry faces in obtaining Federal security clearances. This panel is a positive step forward for creating actionable solutions to challenges that have plagued this process for decades, a process that keeps highly qualified people from working in high paying jobs of national importance. My name is Doug Wagoner, and I serve as chairman of the ITAA Security Clearance Task Group. I also bring the perspective as a small business IT executive from Fairfax struggling with this issue everyday.

As you may know, ITAA is the Nation's leading trade association focused on the IT industry, providing public policy and national leadership to promote its growth. ITAA represents firms large and small, including virtually every major Federal contractor. I have included more detail on ITAA's solutions to this problem in my written statement along with a copy of the detailed White Paper that ITAA and seven other industry associations prepared that provides five recommendations on how to improve this complicated process without sacrificing security.

While the pressures placed on an already stretched system have significantly increased following September 11, the challenges we face have been the same for decades. Since the 1980's, Congress, the executive branch, and GAO have been looking at the problem with no reformed policy to make substantive changes. The Government rightfully demands high standards from its contract personnel, and ITAA does not want to reduce the standards to obtain a clearance. National security is priority one for industry.

I would like to focus on three main issues in ITAA's recommendations to improve this process. ITAA recently completed a survey of its membership on clearances and I will highlight the results in this statement.

The first issue is with consistently elongated time to grant initial clearances. As with NVTC, 70 percent of respondents state that it is taking more than 270 days to obtain a top secret clearance, and that is for a clean case, and 16 months for those needing more extensive investigations or polygraph. These delays are costing people jobs. Almost 22 percent of our survey respondents had over 500 open positions right now, and 70 percent are saying that they have seen significant increase in the need for these cleared personnel over the last 5 years. With an increasing demand and a constrained supply, industry is poaching employees where they can, sometimes paying referral bonuses of up to $10,000 per cleared person. Fifty-three percent of our respondents state that they primarily recruit cleared personnel away from other contractors, 10 percent say they primarily hire away from Government. That means almost two-thirds of the cleared people industry hires leave another cleared opening to be filled. Government has created a zero-sum game that creates instability in critical programs and drives up cost to both industry and Government, as I will discuss in more detail.

ITAA recommends several solutions. First, we recommend that agencies work through the procurement process to authorize bench strength of cleared personnel. An example of this is if a contract requires 20 cleared slots, we recommend that procurement officials authorize 24. These ready replacements would ensure that critical programs stay on schedule and do not get bogged down because of staff turnover. An industry-wide bench strength would also increase the supply of cleared people, removing the zero-sum game and price pressures.

Second, ITAA would recommend that a statutory performance metric of 120 days be established to complete a top secret clearance, and that a Government industry advisory panel be tasked to create the policies and reforms to achieve that metric. Standardization and reciprocity are also enormous issues. ITAA has identified more than 20 agencies in the Federal Government that have clearance requirements and most with unique items of inquiry. Often a clearance is granted at one agency that will not be recognized by another. For example, at DOJ, a DEA clearance is not honored by FBI, and vice versa, because of different requirements even though they are within the same Department. This also creates problems for our first responders who need multiple clearances to share information with the Federal Government. It would seem logical, Mr. Chairman, that when one Federal agency grants you a clearance it should be honored by all of government to work at the same security level.

ITAA recommends that a consistent baseline requirement be established across Government to specify data requirements and investigation methods. The Defense Science Board could also be tasked to create policies governing security clearances for the defense and intelligence community.

Cost is the third issue that we need to consider. High demand and low supply of cleared people is rapidly increasing labor costs. Over half of the people in our survey said that they pay up to 25 percent more for a cleared employee who performs the same job as an employee without a clearance. This, coupled with increased recruiting costs, creates higher costs for Government in the form of higher labor rates and contract delays due to unstable work force. Clearance delays significantly affect a company's ability to grow. Twenty-two percent of our survey told us that the clearance process alone impacts annual revenue by $10 million. It has prevented the growth in my small business by 20 percent this year. GAO has estimated the cost to Government in the billions of dollars annually. But more importantly, Mr. Chairman, GAO and others have pointed to direct risks to national security. It is clear that business as usual cannot continue. Changes to policy, technology, and management processes must exist to reform this antiquated process.

Two final snippets from our survey. Ninety-six percent told us that if Government could issue a top secret clearance in 120 days or less, they could better serve the national security needs. And 85 percent told us it would be easier to bring the best and the brightest to Government if we could get that 120-day mark.

ITAA members value their partnership with Government and are committed to improve this process that is critical to national, economic, and personal security. Thanks again for your invitation, and I am happy to answer your questions.

[The prepared statement of Mr. Wagoner follows:]

STATEMENT

OF

Doug Wagoner

Chairman, ITAA Intelligence/
Security Clearances Task Group

BEFORE THE

HOUSE COMMITTEE ON GOVERNMENT REFORM

CONCERNING THE
ISSUANCE OF SECURITY CLEARANCES BY THE FEDERAL GOVERNMENT TO INDUSTRY CONTRACTOR PERSONNEL

ON BEHALF OF

INFORMATION TECHNOLOGY ASSOCIATION OF AMERICA

May 6, 2004



Introduction

Mr. Chairman and Members of the Committee. Thank you for inviting the Information Technology Association of America (ITAA) to testify today on the issues affecting the government contracting community as a result of backlogs, lack of reciprocity, and severe delays in the granting of security clearances that are taking over a year to complete to get someone working on classified government support project. Industry seeks to work with the government to get that time down to 120 days over the next two years. As an association, we would favor a statutory performance metric that will require clearances to be completed in this time frame rather than provisions that would specify how to accomplish the time reductions.

My name is Doug Wagoner, and I serve as Vice President and General Manager of Data Systems Analysts, Inc. (DSA), a small IT services company in Fairfax, Virginia. I'm here today, however, in my role as Chair of ITAA's Intelligence Committee, which was established in November 2002 following consistent calls from the ITAA membership for assistance from their trade association in resolving the tremendous burdens and challenges IT contractors face with this vital component of national security.

As you know Mr. Chairman, ITAA is the nation's leading and oldest trade association focused on the diverse information technology (IT) industry, and provides global public policy, business networking, and national leadership to promote the continued rapid growth of the IT industry. ITAA consists of more than 400 corporate members throughout the United States, and serves as the Secretariat for the World Information Technology and Services Alliance (WITSA), a global network of 50 countries' national IT trade associations. ITAA represents virtually every major federal IT contractor and many other public and private sector contractors, and counts among its membership a wide range of companies from the largest enterprise solutions providers to the smallest IT start-ups. The Association takes the leading role in major public policy issues of concern to the IT industry, including government IT procurement, homeland security, information security, taxes and finance policy, digital intellectual property protection, telecommunications competition, workforce and education, immigration, online privacy protection, and e-commerce, among others.

The federal government continues to rely heavily on commercial industry partners to fulfill critical government services. The sheer magnitude of commercial activities in support of the government necessitates that government and industry work together to ensure the best private sector personnel are available to fulfill critical government needs. In order to perform many of these critical services in partnership with government, industry personnel must obtain and renew security clearances. The current security clearance process, rules, and regulations are very important to industry and create a mechanism that we believe must be improved upon in order to better safeguard the national security by permitting industry to hire and clear qualified personnel in a timely fashion. As we deal with new asymmetrical threats in our ongoing war on terrorism, government's industry partners face increased pressure to deliver cleared personnel on the very day a contract begins. The current delays being experienced by contractors in obtaining security clearances prevents this from happening and as a result, delays performance on critical programs and increases costs to the federal government in the form of higher labor costs and protracted contracts.

It's important that we note as we begin this hearing Mr. Chairman that these challenges and concerns are not new. While the pressures placed on an already stretched system because of heightened security demands following the September 11th attacks certainly have exacerbated the problems in the system, the challenges we face have been the same for decades. In fact, since the early 1980s, if not earlier, the issue has been raised in the Congress, the Executive Branch, and oversight bodies such as the General Accounting Office in the hope that some changes can be made to what is a vastly complicated and highly repetitive process across government. The problem is certainly more pronounced now because of higher demand, but the core challenges remain the same. Industry (and government personnel in need of clearances) is still seeing a more than 12 month time period for the issuance of a new Top Secret DOD clearance – this is the average for a "clean case" where an individual has had limited foreign travel, and has no credit or police problems. Clearances requiring more extensive investigations, including a polygraph, are routinely taking 16 months or more to complete.

Within the ITAA membership, the current delays in obtaining security clearances consistently ranks #1 or #2 among the chief concerns our members have in their ability to effectively do business with the federal government. Since our members businesses are built around partnership with the government, the inability to deliver cleared personnel directly prevents them from meeting critical government missions and priorities. Given the role the IT community plays in enabling digital government and the information sharing that is so vital to government efficiency and homeland security, we believe our members' experience with the challenges in obtaining security clearances represents an accurate model of what other contracting sectors have experienced with this issue. In other ways, our members' experiences represent an even more acutely

important example given the role of information technology in government operations. Quite simply, if our members are unable to meet critical mission needs, the downstream mission areas dependent on information technology will also be hindered.

In addition to the personnel security clearance process delays, the failure of federal agencies and Departments to honor existing regulatory requirements, such as those mentioned in the body of this testimony, causes inordinate and unacceptable delays in moving personnel with existing clearances and special accesses from one contract or supported government customer to another. These actions can and should be accomplished in minutes, not months, simply by adhering to existing regulatory requirements and deploying technologies and management practices that are well developed.

Before I detail ITAA's recommendations to reduce the time to clear both government and industry personnel, I cannot emphasize enough that industry in no way wants to diminish our nation's security posture by reducing the important standards that govern who has access to sensitive government information. My committee worked for the better part of the last year to create these recommendations. The time involved was due in large part to constant review by security experts to ensure our recommendations would not negatively impact security. Industry is committed as a trusted partner of government to safeguarding national security information; we believe, however, that much can be done to improve the current process without diminishing this fundamental goal.

In November 2002, ITAA formed a task force to deal with the increasingly important issue of security clearances. I am honored to serve as the Chairman of this task force, which is comprised of senior executives from ITAA member companies whose collective experiences encompass the full range of industrial and personnel security disciplines. Several members of our task force have served in senior level security positions within the defense and intelligence communities, and most have gone through the clearance process multiple times as part of their government or military service, and now, as industry partners with the government on mission critical programs.

When our task force initially convened, we spent the first several meetings sharing "horror" stories about the process. Without exception, members of our task force were able to recount in remarkable detail untold numbers of bad experiences they have had with getting their personnel cleared to work on specific programs. As we explored the "horror" stories with our members, we also received startling statistics from our members that drove home just how significant a problem this is for industry; time and time again, we were told that particular companies have several hundred or even thousands of positions open that require clearances for which they cannot find suitable cleared candidates to fill in a timely manner.

We will discuss some more formal statistics in greater detail later in our testimony, but these anecdotal stories are reinforced every day here in Washington on our radio waves and in print and television advertising. Ultimately, what this issue comes down to is jobs: there are literally thousands of job opportunities available here and around the country that cannot be filled because there isn't a large enough population of cleared workers. And one of the major reasons there isn't a large enough population of cleared workers is because there also aren't sufficient investigators available to ensure the timely completion of new background investigations. If you've listened to National Public Radio (NPR) or WTOP while you've sat in Washington traffic, I have no doubt you've heard the countless ads played over and over again from local technology companies seeking applicants with current clearances. My company is among those that have turned to the airwaves to solicit cleared personnel.

A current clearance that can be put to work immediately for a company is worth 10 times its weight in gold. If you go to any job fair here in the Washington area and tell recruiters you have an active clearance, you can probably walk out of that event with multiple job offers. Job seekers with active clearances know this, and we're seeing startling trends where employees move from company to company every 6 months because they're lured away by higher salaries from competing companies. Each time the employee moves around, his or her salary may jump 10%-25%; while this is good news for the employee, it significantly increases costs to the company. These costs are most often passed back to the government in the form of higher labor rates for specific employees working on a contract. The associated turnover when employees jump from one company to another also disrupts critical government programs that become short-staffed upon the departure of key personnel.

ITAA has heard for several years a lot of anecdotal information from member companies about the challenges and pains they experience with the security clearance process, but we wanted to make sure we had real statistics to share with you today, so we developed a survey instrument to poll ITAA members with some very specific questions about their experiences with this critical process.

While it is unknown what the total current number of cleared contractor job vacancies is across government, it is clear the number of openings from company to company is staggering. ITAA asked its member companies to identify the number of current openings in their company that require security clearances. Nearly 50% of our survey respondents indicated having less than 50 current openings that require clearances, but a staggering 22% of respondents indicated they have 500 or more positions open that require some level of clearance.

Nearly 70% of respondents indicate that the clearance process is restricting their ability to grow their company; small companies in particular have a difficult time

filling significant numbers of positions in a short time period. Take my company DSA as an example; at the end of last fiscal year, we were fortunate enough to win several contracts we bid for work at DoD and within the Intelligence Community. Our company currently has only about 150 employees. These new contractual obligations required that we hire approximately another 50 individuals. We have purchased advertising on WTOP and tried every other recruiting tactic we know, but as of this hearing, we still have 40 positions open.

On the topic of recruiting methods, the ITAA survey also asked member companies to document how they primarily recruit new talent for work requiring security clearances. Fifty-four percent (54%) of respondents indicate that they regularly recruit individuals with current clearances from other contractors. Another 10% say they recruit employees from government with active clearances, and the remaining 36% say they work to clear existing staff without clearances and deploy them to national security related projects. That means that almost two thirds of employees brought on to programs are ripped from another program they are currently working for another contractor or as a government employee. That statistic clearly defines the need to infuse new cleared talent into the pool.

Our survey data also indicates that employees with an active clearance consistently command salaries that are dramatically higher than their colleagues performing the same job without a clearance; according to our results, 56% of respondents noted that they pay premiums of anywhere from 5% to 25% for cleared workers. Perhaps more glaringly, 70% of our respondents indicate that this premium continues to increase as the demand for cleared workers intensifies. In fact, 60% of our survey respondents indicated that they have seen "significant increases" in the contractual requirements for cleared workers over the past 5 years. In a recent GAO report on the DoD clearance backlog, investigators noted "a growing percentage of all DoD requests for clearances is at the top secret level. For example, in fiscal years 1995 and 2003, 17 percent and 27 percent, respectively, of the clearances requests for industry personnel were at the top secret level" (*GAO-04-344 DoD Personnel Clearances report*, page 15). GAO goes on to note that this increase is significant because clearances at the top secret level must be renewed twice as often as secret clearances, and take eight times as long to investigate and three times as long to adjudicate than clearances at the secret level.

Our survey indicates as well that the time to complete clearances continues to rise. We asked our respondents to tell us how long it takes on average for them to obtain a Top Secret clearance. We asked respondents to take into account both the investigative and adjudicative time periods. Seventy percent (70%) of our respondents noted that it takes on average more than 270 days to obtain this level of clearance. We also asked respondents to answer the same question from a perspective of one and two years ago. Fifty-nine percent (59%) indicated

that the process took more than 270 days a year ago, while 49% told us it took longer than 270 days two years ago.

On average, our survey respondents indicated that nearly 60% of their cleared workforce performs duties on DoD-related contracts. No one denies that DoD is the largest single organization that grants clearances to industry personnel. At the same time, the clearance problem is one that affects all agencies of government. Given the enormous scope of DoD's involvement in this function, we understand the demands placed on DoD to clear the enormous number of individuals, but we believe industry and government must work together to implement a workable solution to reduce the time it takes to secure a clearance and increase the portability of clearances across government agencies.

Our survey results reinforced what we in industry already knew: cleared personnel cost more, there is an increasing need for cleared personnel, and industry hire away cleared personnel from one another with great regularity to decrease the risk that a critical program will miss milestones for lack of adequate staff.

ITAA does not believe the problem lies just with DSS and OPM. The problem is exacerbated by antiquated policy that leadership does not want to address. While we applaud the efforts underway to reform the process, similar initiatives have failed in the past because we are trying to automate a system that needs to be re-engineered to address security realities of today. Similarly, there appears to be a disconnect between the procurement functions and the security functions. Procurement officers generally issue security requirements to contractors, and these requirements generally dictate the number of security "billets" a company is required to hold, and the security level for each of those billets. It is great that DSS can issue an interim secret clearance in 3 to 5 days, but the problem is that industry has very few contracts that have been designated at that level. Part of the reform of the security clearance process, we believe, must include an examination of how security clearance levels are set and approved during the procurement phase of a project.

ITAA has led the formation of a diverse coalition of trade associations to develop joint recommendations on how to improve the current process. This coalition has produced a white paper, which I attach to my testimony today and ask to be included in the official hearing record. Joining ITAA on this industry white paper are seven other prominent trade associations that represent the broad spectrum of the government contracting community:

- The Security Affairs Support Association (SASA);
- The Professional Services Council (PSC);
- The National Defense Industrial Association (NDIA);
- The Contract Services Association (CSA);
- The Northern Virginia Technology Council; (NVTC)

- The Armed Forces Communications and Electronics Association (AFCEA); and
- The Electronic Warfare & Information Operations Association, more commonly known as the Association of Old Crows (AOC).

Together, these organizations represent thousands of companies and tens of thousands of individuals with diverse responsibilities across the security and defense spectrum: from IT services, to manufacturing and engineering, and from complex services offerings, to weapons development and modernization. Working together, these industry associations have developed five specific recommendations to improve the security clearance process, improve the nation's security posture, better enable our members to serve their customers, and lower the cost to government. The changes we recommend in this white paper, we believe, would have a significant impact on the ability of people to obtain, hold, and maintain their clearance status and will ensure that critical government programs do not go unexecuted for lack of available cleared personnel. I will present these recommendations in summary form here, as the white paper covers these issues and recommendations in much greater detail, and will also cover some additional issues ITAA has concerns with that are not specifically addressed in the white paper.

SPECIFIC RECOMMENDATIONS FROM ITAA

Much of the debate of late, Mr. Chairman, surrounding the issue of security clearances has focused on the transfer of investigative functions of the Defense Security Service to the Office of Personnel Management that was authorized as part of the FY 2004 Defense Authorization bill. Many have pointed to this authorized transfer as the prescription to solve the long delays and process challenges inherent to this process. As GAO and others have noted, however, the potential transfer has been slow to proceed. Industry is concerned both with the delays in a potential transfer, and with the notion that this transaction will somehow miraculously improve the current process. While there will be advantages in moving to a single case management system at OPM, ITAA believes little will actually change without significant reform of the processes that underlie the current program. Moving the responsibility for investigations from one entity to another will do little to fundamentally change the process.

In fact, we understand that as a result of the impending merger of DSS and OPM, a large number of security clearance investigations submitted to DSS since the start of the fiscal year remain unopened. Of the estimated 100,000 cases in this category, a substantial number represent defense industry personnel. This situation only exacerbates the problems we have identified above in filling vacant contractor positions in a timely manner with cleared personnel. GAO has pointed out that OPM will increase its annual investigative caseload by nearly 800,000 cases when the merger with DoD takes effect. This increase in caseload will tax an already over-burdened system, and industry is

concerned that this situation could result in even greater delays in the issuance of clearances.

As we look to solutions, ITAA believes it is important to support the Office of Management Budget and Office of Personnel Management e-Clearance initiative as a means to reduce backlogs in issuing clearances. While the work done as part of the e-Clearance initiative is helpful in increasing timely access to existing clearances and automating the paperwork requirements to apply for a clearance, we believe much more needs to be done to reform the process and get cleared workers deployed to critical contracts and support functions more quickly. Specifically, ITAA recommends:

- That federal agencies examine issues relating to procurements and recommend corrective actions to allow for 'Bench Strength' on contracts requiring security clearances;
- That data requirements and clearance processes be standardized across federal agencies to provide for uniform baseline standards all agencies recognize for like levels of clearances;
- That reciprocity (or crossover) for clearances from agency to agency be dramatically increased so like clearance levels can be applied to any agency in government;
- That agencies work with the private sector to address the current investigative and adjudication backlog by employing a coordinated approach that leverages private sector expertise and information technology to speed investigations and adjudications. Specifically, we recommend that government examine the use of commercially available databases to reduce investigative demands and establish on-going monitoring for adverse events to reduce the need for periodic reinvestigations;
- That Congress request the Defense Science Board to immediately review policies governing security clearances and make recommendations for changes, including recommendations on changes in the procurement-related aspects of clearance requirements; and
- That Congress support and fully fund OMB's and OPM's e-Clearance Initiative.

We believe that the changes recommended here would have a significant positive impact on the ability for people to obtain, hold, and maintain their clearance status. And we believe that an improved process would open new opportunities for people seeking employment in sensitive private sector specialties.

The recent stand-up of the Department of Homeland Security presents new opportunities to address how this process functions at a new agency during its foundational stages. As DHS continues to integrate the operations of the 22 disparate legacy agencies that comprise it, we have a good opportunity to fix

what's wrong before the process gets too ingrained in the culture of the Department. The process so far within DHS has been slow, but I think everyone in the contracting community is willing to give DHS more time to deal with the issue given their nascent stage. It's important to note, however, that in their brief time of existence, the clearance issue has been raised in several instances in the context of other oversight hearings. At a hearing of the House Select Committee on Homeland Security last year, for example, witnesses testified about significant delays in the granting of security clearances to airport screeners and state and local first responders. ITAA's membership also fulfills critical services for this community and has significant concerns about how delays in granting clearances for contractor personnel affect this unique community. Access to a government-wide clearance database like the Joint Personnel Adjudication System (JPAS) and full implementation of security clearance reciprocity would reduce the time first responders wait to obtain clearances and make it easier for these critical components of our national security to work in better collaboration with the federal government. Faster clearance times would also ensure that contractor personnel supporting critical first responder missions receive timely classified information that is transmitted to the user community.

AGENCIES SHOULD ALLOW FOR "BENCH STRENGTH" ON CONTRACTS REQUIRING SECURITY CLEARANCES

The current clearance process across all agencies requires that clearances be granted only to those currently assigned to projects or contracts requiring a clearance. Industry would recommend that agencies be permitted to clear up to 20% of additional industry personnel. Under most contracts, industry is told how many billets they need to fill by way of the RFP or information received from contracting officers. Many federal security officers report that they are then constrained by the number of billets allocated by a contracting officer to a particular contract. If an individual leaves the company that has that contract, or the company needs to rotate that person to another contract they are working on, a slot opens up on the contract that needs to be filled. Unless the company has a ready staple of cleared personnel who can immediately step in at that particular agency at the correct clearance level, the company is usually forced to start the process for a new employee all over again. ITAA recommends that agencies move toward allowing bench strength by first educating the procurement workforce across the government on the critical issues that arise from the limited cleared slots currently provided for in federal contracts.

Providing for bench strength would bring benefits to government and industry in that the increased supply of cleared people would bring down the cost to government and industry would be able to ensure the best people are working a project as opposed to only those who simply "hold a clearance." The creation of 'bench strength' of cleared people would also enhance national security, as there would be a pool of individuals readily available to address critical missions. We

believe this is also a critical requirement to limit the spiraling salaries of employees with clearances, a cost that ultimately is paid by the government.

An additional consideration is the aging government workforce. As these seasoned government workers retire, even more demands will be placed upon contractors to supply cleared quality personnel. Industry would be willing to look into sharing the cost of creating this bench strength, following the precedent of paying for expedited investigations at the National Security Agency (NSA).

GOVERNMENT SHOULD STANDARDIZE DATA REQUIREMENTS AND INVESTIGATIVE PROCESSES FOR LIKE SECURITY CLEARANCES

All security clearance processes ultimately assess a core set of investigative data. For example, most clearance processes examine a subject's identity data, address history, employment history (including military service record), educational achievement, financial status, and personal references, with the additional requirement for a National Agency Check for derogatory information (i.e., criminal history, intelligence or other government data) that would increase risk. The commonality of the data required for clearances creates the opportunity to standardize collection and assessment of that data across the government.

ITAA envisions that the standardization process would start with identifying data elements and investigation processes common to all clearances to set a "baseline" background investigation. That baseline could then provide the foundation for a tiered structure of security levels to correlate to the level of trust required and consequences of a breach of trust for categories of missions, operations, functions or facilities. The government could accommodate different levels of security by varying the breadth and depth of the investigation or the rigor of the adjudication criteria, as well as assessing additional elements of the applicant's background beyond the baseline.

The baseline, however, would apply as the minimum standard for the lowest level security clearance in the context of any government operation – civilian, defense or intelligence. Higher levels of clearance would require a more intensive inquiry (e.g., longer historical perspective, polygraph) or assessment of additional elements of the subject's background (e.g., "life style" queries). Standardizing data and process requirements at each tier for clearance levels across operations with common risk profiles (i.e., law enforcement, homeland security, defense, intelligence, etc.) across the government would yield tremendous efficiencies to reduce time and cost of administering clearances while increasing the effectiveness in maintaining security.

Establishing a common baseline would also reduce the need for multiple application, investigation and adjudicatory processes, which in turn would minimize requirements for specialized training and certification of investigators and adjudicators. Standardization also would facilitate implementation of the

OMB/OPM e-Clearance initiative and promote centralized administration of clearance information government-wide.

At the same time, industry believes that by granting immediate access to industry to databases like DoD's JPAS and the Office of Personnel Management's Clearance Verification System (CVS), industry can make quantum leaps in its ability to quickly and efficiently transfer clearances with little or no cost or delay. Currently, when an employee leaves ABC Company to go to work for XYZ Company it can take over four weeks, as contractors wait for a government agency to transfer for the paperwork between parties. A common database approach like JPAS/CVS will ensure that each agency is able to effectively share clearances in the fastest possible manner. DSS has begun this process with the larger firms and is now making its way to small businesses.

In addition to efficiencies in the initial clearance process, standardization would facilitate transferability and ongoing administration of clearances from one agency to another or even across levels of government. Operating from a standard baseline would streamline and expedite the process of adjusting clearance levels or clearing individuals for new missions by enabling investigators to focus only on updating the baseline and/or evaluating additional elements beyond the baseline as opposed to repeating the entire process from scratch. In addition, development of standard structure of security clearance requirements could some day facilitate a system to monitor the continuing validity of clearances. The government could enroll all individuals holding a specified clearance in a database to monitor available public and government records for changes in status (e.g., arrest, bankruptcy, unexplained affluence, etc.) that might indicate a potential security risk.

In fact, the DoD has developed and tested such a system, the Automated Continuing Evaluation System (ACES), which is low cost and can be deployed in six months if final funding is approved. The ACES monitoring system, using advanced techniques, will identify and flag specific risk factors as defined in the applicable security rules based on near real-time searches of approximately two-dozen government and commercial databases.

Early deployment of ACES would provide the government with much earlier and cost effective warning of potential security issues than the current reinvestigation process alone, and would also reduce reinvestigation time, thereby freeing up resources to pursue investigative functions on new clearances. Standardizing clearance criteria and processes with an ongoing monitoring process, along with an accurate and reliable clearance database, will enable security officials to have greater confidence in clearances conducted for other agencies, facilitating transfer and acceptance of security clearances across the government.

In four Departments and agencies within the intelligence and defense community that we examined, we found four different standards and processes for

clearances. Industry would recommend that the process be reconciled between the largest organizations. At an absolute minimum, industry would propose that the DOD, NSA, CIA, and NRO work to reconcile their data requirements and processes for investigations and adjudication in line with the recommendations made above. In conjunction with a statutory performance metric to get clearances issued within 120 days, we would recommend the appointment of a joint working group to develop standardized processes across the government. We believe that industry should be represented on this panel as well. ITAA believes that another potential solution would be to task the Defense Science Board to present specific recommendations to the Secretary of Defense on how to improve the current process. The last thing we need is another study on the problems we're facing. What we need are solutions, and as you know Mr. Chairman, the Defense Science Board's recommendations are actionable.

GOVERNMENT MUST PROVIDE FOR INCREASED RECIPROCITY FOR CLEARANCES ACROSS FEDERAL DEPARTMENTS AND AGENCIES

Much like the lack of standardization in clearance requirements, there is currently little reciprocity among federal agencies to honor a clearance granted by another federal Department, even when at the same level. It would seem rational to argue that when one federal agency grants you a top-secret clearance, that clearance should be honored by any other government agency that requires you to have clearance at the same level, provided the investigation remains current. Sadly, however, this goal is hardly ever realized, despite the existence of Executive Orders from multiple administrations requiring greater standardization of criteria and portability. Even within individual government agencies we've found unique processes for clearances at the same levels. In fact, examples of intra-Departmental battles over clearance levels abound; within the Department of Justice prior to the stand-up of DHS, for example, a clearance held at the Drug Enforcement Administration might not be honored by the Federal Bureau of Investigation, and vice versa, because of different criteria to get those clearances.

ITAA has identified more than 20 distinct processes across the federal government; each process has its own special requirements that go beyond or are unique from other agencies. These requirements prohibit one agency from honoring the same level of clearance from another agency. ITAA would recommend that a baseline requirement be created by the advisory body we recommend above to indicate that in accordance with uniform standards, no federal agency will reinvestigate an individual who holds an active clearance at the required security level from any other federal agency, again, provided that the investigation is current. While there may be additional criteria to be examined, the baseline level of clearance should be accepted and agencies shouldn't repeat an entire investigation on someone who has undergone the same review for another agency.

Industry would also like to have authority to transfer clearances between each other on a near real-time basis. This relates to the situation when an employee leaves ABC Company to go to work for XYZ Company. Member firms of the ITAA coalition have documented that this simple process varies dramatically by agency, and can take over four weeks, as contractors wait for a government agency to transfer the paperwork between parties. A common standard and approach to sharing clearances should be developed to ensure that each agency has the same standards and is able to effectively share clearances in the fastest possible manner.

GOVERNMENT MUST ADDRESS THE CLEARANCE BACKLOG BY PARTNERING WITH INDUSTRY AND LEVERAGING INFORMATION TECHNOLOGY TO IMPROVE PROCESSES AND MANAGEMENT

ITAA certainly applauds the growing use of private sector investigative providers to help conduct background investigations; however, even with the use of the private sector, the increased numbers of clearances being requested is extending the backlog that already exists and resulting in even longer delays at both the investigative and adjudicative ends of the process. Based upon our member's experience, there is an increasing adjudicative backlog as more investigations are being completed and overwhelming the available adjudicative workforce. In its recent report to the Armed Services Committee, GAO pegged the current backlogs at DoD alone at nearly 360,000.

Information technology has transformed government services in countless ways. As we continue the e-Government revolution that has already modernized so many antiquated government programs, ITAA believes that the power of information technology can do much to improve this vital process as well. In addition to recommending support for existing e-Government initiatives, ITAA also would note that reliable commercially available technologies like public records databases can play a vital role in verifying information submitted by applicants for clearances. Several highly respected companies already support major corporations in their employment pre-screening and risk management processes by offering databases that can help verify whether an individual has had financial problems such as liens or judgments, whether the individual has a criminal history that would disqualify them from receiving a clearance, and whether the individual in fact lived at a location they claim on an application. These applications can dramatically reduce the need for field agents to spend valuable time pounding the pavement interviewing friends and co-workers of the individual under investigation. Clearly the role of field investigators cannot be done away with; there is vital information discovered in personal interviews with subjects who know an individual well. We do believe, however, that the power of information technology can vastly improve the length of this process without compromising security.

IMPLEMENT/FUND THE OFFICE OF PERSONNEL MANAGEMENT'S E-CLEARANCE INITIATIVE

ITAA endorses the Office of Personnel Management's (OPM) e-Clearance initiative. The concept of e-Clearance, such as sharing resources on-line, whether for information collection, information review, or adjudication, including sharing among interested agencies, can help transform and speed the clearance process by reconciling and harmonizing the existing disparate clearance procedures. While the automation of standard clearance forms and the establishment of a central database of existing clearances should help the process, the coalition recommends that the e-Clearance initiative also address the shared data and process issues identified in our testimony. We recommend that Congress provide full funding and support for the e-Clearance initiative in annual appropriations.

Conclusion

I cannot emphasize enough Mr. Chairman that industry is committed to preserving the strict requirements to obtain security clearances. The coalition's interest is not to minimize current requirements, but rather, to make sensible and positive changes to an antiquated process and policy that would allow the nation to maintain strong vigilance on who has access to data, while better serving the defense and intelligence communities at the lowest possible total cost. Involving the Defense Science Board to review and make recommendations to this problem would be a good first step. Industry looks forward to working with the government to examine and implement the recommendations we make today to move the average top secret clearance form 12 months to 120 days. We stand ready to devote our experience and significant expertise with best practices to ensure that critical government programs do not go unexecuted for lack of available cleared personnel, and we look forward to growing our companies by adding many new employees with highly skilled and compensated new jobs. Thank you Mr. Chairman for the opportunity to appear before the Committee today. I would be happy to answer any questions from you or other members of the Committee.

Improving the Security Clearance Process Through Automation and Common Criteria:

A White Paper on Issues Confronting the Government Contractor Community

Prepared by

Information Technology Association of America
Professional Services Council
Security Affairs Support Association
Contract Services Association
Armed Forces Communications and Electronics Association
National Defense Industrial Association
Northern Virginia Technology Council
Association of Old Crows















EXECUTIVE SUMMARY

The federal government continues to rely heavily on commercial industry partners to fulfill critical government services. Recent studies have suggested that as many as 850,000 government jobs are commercial in nature. The magnitude of commercial activities necessitates that government and industry work together to ensure the best private sector personnel are available to fulfill critical government services. In order to perform many critical services, industry personnel must obtain and renew security clearances. The current security clearance process, rules, and regulations are very important to industry and create a mechanism that we believe must be improved upon in order to better safeguard the national security by permitting industry to obtain and clear qualified personnel in a timely fashion. Industry faces increased pressure to deliver cleared personnel on the day a contract begins, and the current delay in obtaining security clearances increases costs to the federal government by delaying the introduction of the best personnel to critical programs.

Elongated clearance processes adversely affect mission accomplishment, keep people from working in a productive and timely manner, and add to the cost of contractor programs to the federal government. Members of several industry associations have developed four specific recommendations to improve the security clearance process, improve the nation's security posture, better serve our customers, and lower the cost to government. The changes recommended here would have a significant impact on the ability of people to obtain, hold, and maintain their clearance status and will ensure that critical government programs do not go unexecuted for lack of available cleared personnel.

With the growing backlogs and investigative delays being experienced by the Intelligence Community, Defense Security Service and the Office of Personnel Management, it can take more than a year to process a new employee for a background investigation and a security clearance. Even new employees with prior investigations and security clearances can wait weeks for their clearance to be converted or reinstated by the government. While all this "lost" time is not completely non-productive, in some cases the employee cannot be of full value to the contract and customer without his or her final security clearance; in most cases, it prevents the hiring of qualified people.

BACKGROUND

The Information Technology Association of America (ITAA) along with partner organizations including the Professional Services Council (PSC), Security Affairs Support Association (SASA), Contract Services Association (CSA), Armed Forces Communications and Electronics Association (AFCEA), Northern Virginia Technology Council (NVTC). National Defense Industrial Association (NDIA), and the Association of Old Crows (AOC) (collectively, "the coalition") present this paper on the current state of the security clearance process for contractors. The collective membership of these

organizations is drawn from the leading technology firms in the United States. These companies develop and deploy the technology products and services that have helped to make the United States' intelligence and war fighting capability the best in the world.

In order to serve their defense and intelligence clients, our members are required to obtain appropriate security clearances for their facilities and employees. The security clearance process, rules, and regulations are of vital interest to industry and create a process that we believe must be improved upon in order to better safeguard the national security. While much has been done since the Eisenhower administration in both policy and procedural areas to try and standardize and simplify the government's personnel security program and promote the notion of clearance reciprocity, in practice it has simply failed to achieve the stated goals and objectives, leaving industry to the mercy of a diverse bureaucracy that is slow to embrace change and eager to protect its "rice bowls." Industry faces increasing pressures to deliver cleared personnel on the day a contract begins, and the current delays in obtaining security clearances limits competition and increases costs to the federal government by delaying the introduction of the best personnel to vital programs and slowing the initiation of critical programs.

As the Bush administration seeks to provide greater competition with the private sector to perform functions inherently commercial in nature, it is critical that the current clearance process be streamlined and improved. The elongated clearance process is delaying missions from being completed in a timely fashion, keeping people from working, and adding to the cost of contractor programs to the federal government. In today's clearance process, it is virtually impossible to share a good idea or leverage an existing team between agencies. It is unknown what the total current number of cleared contractor job vacancies is across government, but one program alone at NSA is said to have more than 400 openings. The current clearance process prevents thousands of vacant positions requiring a security clearance from being filled in a timely manner. Given the critical role that the Intelligence Community agencies play in securing the national security of the United States, we must fill these and other critical positions with cleared, skilled people as soon as possible. The post September 11th increase in the need to clear and hire staff in all agencies has added to the investigative and clearance backlog problem and we must conclude that a considerable amount of important work is not getting done. While the agencies strive to fill these critical positions, programs requiring cleared contractor personnel suffer as a result of growing investigative and clearance backlogs as well as bureaucratic impediments and opposition to implementation of clearance reciprocity policies that were enacted in Executive Order 12968 following the Ames espionage case.

Recent studies conducted under the Federal Activities Inventory Reform (FAIR) Act suggest that as many as 850,000 government jobs are commercial in nature. The magnitude of commercial activities necessitates that government and industry work together to ensure the best private sector personnel are available to fulfill critical government services.

RECOMMENDATIONS

In principle, the coalition supports the Office of Management and Budget's and Office of Personnel Management's e-Clearance initiative as a means to reduce backlogs in issuing clearances. There are also four recommendations that we believe will improve our security posture, better serve our customers, and lower the cost to government. These are:

- That agencies allow for 'Bench Strength';
- That agencies address the current investigative and adjudication backlog,
- That there be increased reciprocity for clearances from agency to agency; and
- That data requirements and clearance processes be standardized across agencies.

We believe that the changes recommended here would have a significant positive impact on the ability for people to obtain, hold, and maintain their clearance status. An improved process would open new opportunities for people seeking employment in sensitive private sector specialties; as recently documented in one *Washington Post* article, a northern Virginia contractor has over 70 openings but can't fill the positions due to a lack of cleared people or the cost to the company of hiring and waiting up to eighteen months for their clearances to come through.

A July 2003 hearing of the House Select Committee on Homeland Security also uncovered significant delays in the granting of security clearances to airport screeners and state and local first responders. The coalition's membership also fulfills critical services for this community and has significant concerns about how delays in granting clearances for contractor personnel affect this unique community. Access to a government-wide clearance database and full implementation of security clearance reciprocity would reduce the time first responders wait to obtain clearances and make it easier for these critical components of our national security to work in better collaboration with the federal government. Faster clearance times would also ensure that contractor personnel supporting critical first responder missions receive timely classified information that is transmitted to the user community.

Since the current process dictates that security clearances can be held only by individuals who have a bona fide need for access and are employed in a job requiring a security clearance, the Government's process is collectively reducing the supply of cleared staff at a time when the need is increasing. This supply and demand effect is resulting in large increases in salaries of people holding clearances and cleared personnel are moving between employers that are anxious to fill agency openings with cleared people. Because of the costs associated with obtaining security clearances, currently cleared personnel command salaries on average 5% to 10% higher than those for non-cleared personnel according to industry estimates. This cost is most often passed on to the government.

The recommendations from the coalition are detailed below to improve processes to greater benefit the missions of our customers and the security of the United States.

One agency CIO recently commented that the current security process has created a "pseudo society" of people: "These people remain employed not because they work hard, bring innovation, or have the most current skills. They are maintained and even bestowed gracious pay and perks because of their clearance. We need to eliminate this pseudo society and make their contribution the most important factor."

ALLOW FOR "BENCH STRENGTH"

The current security process across all agencies requires that clearances be granted only to those currently assigned to projects or contracts requiring a clearance. Industry is recommending that agencies be permitted to clear additional industry personnel, up to 20 percent of their current cleared population. This would bring benefits to government and industry in that the increased supply of cleared people would bring down the cost to government and industry would be able to ensure the best people are working a project as opposed to only those who simply "hold a clearance." The creation of 'bench strength' of cleared people would also enhance national security, as there would be a pool of individuals readily available to address critical missions. We believe this is a critical requirement to limit the spiraling salaries of folks with clearances, a cost that ultimately is paid by the government.

While the coalition understands that increasing currently cleared personnel may increase investigative and adjudication workloads in the short-term, increasing the supply of cleared resources will benefit the government in three ways. First, it will increase supplies and lower costs long term. Second, the ability for a new or expanded project to get underway quickly will be immensely enhanced. Lastly, an increased pool of resources will make it easier to place quality personnel; it will be much easier to replace people in particular and contractors in general if a larger supply of cleared resources exists.

An additional consideration is the aging government workforce. As these seasoned government workers retire, even more demands will be placed upon contractors to supply cleared quality personnel. Industry would be willing to look into sharing the cost of creating this bench strength, following the precedent of paying for expedited investigations at NSA.

ADDRESS THE ADJUDICATION BACKLOG

While the coalition applauds the growing use of private sector investigative providers to help conduct background investigations, we are seeing an increased delay in adjudication timelines. Adjudication, until relatively recently, has been considered an inherently governmental function. Based upon our member's experience, there is an increasing adjudicative backlog as more investigations are being completed and

overwhelming the available adjudicative workforce. Based on successful outsourcing of adjudicative support functions in the Department of State, Department of the Navy and BCIS (former INS) the coalition recommends that the government make greater use of contract adjudicator support functions until backlogs are eliminated and clearances can be issued or reinstated in 30 days or less.

INCREASED RECIPROCITY FOR CLEARANCES

There is currently little reciprocity of security clearances in the federal government. This is one reason why there is little sharing of information and best practice ideas across the community. Lack of sharing clearances prevents the best and brightest serving one agency to quickly move to solve a similar problem at a different agency.

The coalition would like to create a process where they are allowed to easily move people in a shared clearance process. The lack of sharing between agencies causes problems for employee and employer when a project comes to an end. Once a person is 'read off' of an agency and there is no immediate need for him/her to have a clearance then it is likely they will lose this clearance. If they need to go back to the agency or are transferred to work at another agency a few weeks later, the reinstatement or reinvestigation can take months. With greater sharing there is a much better chance the employee could be moved to another cleared project supporting a different agency.

Similarly, industry would like to be able to have authority to transfer clearances between each other. This is the situation when an employee leaves ABC Company to go to work for XYZ Company. Member firms of the coalition have documented that this simple process varies dramatically by agency, and can take over four weeks, as contractors wait for a government agency to transfer for the paperwork between parties. A common standard and approach to sharing clearances should be developed to ensure that each agency has the same standards and is able to effectively share clearances in the fastest possible manner. The benefits of this approach would also improve the ability of our nation's first responders to work with federal agencies.

STANDARDIZE DATA AND PROCESSES FOR LIKE SECURITY CLEARANCES

While security clearance processes vary across the government with different missions, operational, functional and policy requirements, all of the processes ultimately assess a core set of investigative data. For example, most clearance processes examine a subject's identity data, address history, employment history (including military service record), educational achievement, financial status, and personal references with the additional requirement for a National Agency Check for derogatory information (i.e., criminal history, intelligence or other government data) that would increase risk. The commonality of the data foundation for clearances creates the opportunity to standardize collection and assessment of that data across the government.

The standardization process would start with identifying data elements and investigation processes common to all clearances to set a "baseline" background investigation. That baseline would provide the foundation for a tiered structure of security levels to correlate to the level of trust required and consequences of a breach of trust for categories of missions, operations, functions or facilities. The government could accommodate different levels of security by varying the breadth and depth of the investigation or the rigor of the adjudication criteria as well as assessing additional elements of the applicant's background beyond the baseline. For example, the baseline would apply as the minimum standard for the lowest level security clearance in the context of any government operation – civilian, defense or intelligence. Higher levels of clearance would require a more intensive inquiry (e.g., longer historical perspective, polygraph) or assessment of additional elements of the subject's background (e.g., "life style" queries). Standardizing data and process requirements at each tier for clearance levels across operations with common risk profiles (i.e., law enforcement, homeland security, defense, intelligence, etc.) across the government would yield tremendous efficiencies to reduce time and cost of administering clearances while increasing the effectiveness in maintaining security.

Establishing a common baseline would reduce the need for multiple application, investigation and adjudicatory processes, which in turn would minimize requirements for specialized training and certification of investigators and adjudicators. Standardization also would facilitate ongoing initiatives to implement an "e-clearance" process and promote centralized administration of clearance information government-wide, i.e. JPAS/CVS. Increasing sharing of clearance information and reducing the time and resources required to complete low level clearances will enhance security by enabling the government to allocate more of its limited investigations and adjudication resources to clearances with the greatest sensitivity and highest priority.

By granting immediate access to industry to databases like DoD's Joint Personnel Adjudication System (JPAS) and the Office of Personnel Management's Clearance Verification System (CVS) the coalition believes a quantum leap in industry's ability to quickly and efficiently transfer clearances with little or no cost or delay involved will result. Currently, when an employee leaves ABC Company to go to work for XYZ Company it can take over four weeks, as contractors wait for a government agency to transfer for the paperwork between parties. A common database approach like JPAS/CVS will ensure that each agency is able to effectively share clearances in the fastest possible manner. The benefits of this approach would also improve the ability of our nation's first responders to work with federal agencies.

In addition to efficiencies in the initial clearance process, standardization would facilitate transferability and ongoing administration of clearances from one agency to another or even across levels of government. Operating from a standard baseline would streamline and expedite the process of adjusting clearance levels or clearing individuals for new missions by enabling investigators to focus only on updating the baseline and/or evaluating additional elements beyond the baseline as opposed to repeating the entire

process from scratch. In addition, development of standard structure of security clearance requirements could some day facilitate a system to monitor the continuing validity of clearances. The government could enroll all individuals holding a specified clearance in a database to monitor available public and government records for changes in status (e.g., arrest, bankruptcy, unexplained affluence, etc.) that might indicate a potential security risk. In fact, the DoD has developed and tested such a system, the Automated Clearance Evaluation System (ACES), which is low cost and can be deployed in six months if final funding is approved. The ACES monitoring system, using advanced data-mining techniques, will identify and flag specific risk factors as defined in the applicable security rules based on near real-time searches of approximately two dozen government and commercial databases. Early deployment of ACES would provide the government with much earlier and cost effective warning of potential security issues than the current reinvestigation process alone, and would also reduce reinvestigation time, thereby freeing up resources to pursue investigative functions on new clearances. Standardizing clearance criteria and processes with an ongoing monitoring process, along with an accurate and reliable clearance database, will enable security officials to have greater confidence in clearances conducted for other agencies, facilitating transfer and acceptance of security clearances across the government.

In four Departments and agencies examined by the coalition within the intelligence and defense community, we found four different processes for clearances. Given that there are more than 20 agencies and departments that require clearances, there are likely 20 unique processes. Industry would recommend that the process be reconciled between the largest organizations. Industry would propose that, at a minimum, the DOD, NSA, CIA, and NRO work to reconcile their data requirements and processes for investigations and adjudication in line with the recommendations made above.

IMPLEMENT/FUND THE OFFICE OF PERSONNEL MANAGEMENT'S E-CLEARANCE INITIATIVE

The coalition endorses the Office of Personnel Management's (OPM) e-Clearance initiative. The concept of e-Clearance, such as sharing resources on-line, whether for information collection, information review, or adjudication, including sharing among interested agencies, can help transform and speed the clearance process by reconciling and harmonizing the existing disparate clearance procedures. While the automation of standard clearance forms and the establishment of a central database of existing clearances should help the process, the coalition recommends that the e-Clearance initiative also address the shared data and process issues identified in this paper.

CONCLUSION

It cannot be overstated that industry is committed to preserving the strict requirements to obtain security clearances. The coalition's interest is not to minimize current

requirements, but rather, to make changes to an antiquated process that would allow the nation to keep vigilance on who has access to data, while better serving defense and intelligence at the lowest possible cost. Industry looks forward to working with the government to examine and implement the recommendations made in this white paper, and stands ready to devote its experience and significant expertise with best practices to ensure that critical government programs do not go unexecuted for lack of available cleared personnel.

Chairman TOM DAVIS. Thank all of you for your testimony and for some very specific recommendations for what we might do. It is incredible to me that the representatives from the Federal Government did not have specific recommendations except to keep studying, when you have given I think some fairly quick fixes and which everybody identifies as being human capital, manpower related. I am not sure as followup to this we ought to insist on DOD sitting down with a group of contractors, understanding what these problems are; everybody is talking about it but there is no communication.

DOD has told us about some clearance facilitation programs that it says assists industry contractors. Some of these include the ability to apply for security clearance up to 180 days before an employee starts a job, quick turnaround on interim secret and top secret clearances, and nearly automatic transfers of clearances when an employee moves from one job to another. That is what they testify is working. Does this work?

Mr. SHENOY. Right now, based on the testimony that the lady gave, I think it is mathematically impossible for them to meet some of those goals they have. For example, the 75 days for a secret clearance, by my calculation, they have a little over 4,000 people who do these investigations, there were 86,700 cases pending, which means that it is an average of 22 cases per investigator, and if they take even 15 days per case, each of those investigators have over 330 days worth of work. So which means that after the fifth person has been cleared, the rest are all going to be outside that range.

Chairman TOM DAVIS. You also made a good point I think in your testimony that some of the work that is required for secret clearances and top secret clearances does not really need to be designated that way. The Government could get this job done, they could get the product done at lower cost to them, higher quality product by not requiring this. So are they going overboard on what is required as secret?

Mr. SHENOY. One of the problems I think is in the definition of what secret and what top secret constitutes. My company has clearances with various agencies and every time we get another project which has certain level of clearance, that agency may not accept the other agency's clearance. On one occasion I asked the investigator who was there who had come to interview me about one of my employees, I said, "Why do you need to do this again?" And he explained to me that what is top secret at a particular agency may not be top secret at another one, so that is the reason why they have to redo the investigations. I think what we need is a Government-wide definition of what secret is and what top secret is. I do not believe that exists.

Chairman TOM DAVIS. Does the contractor decide if it is going to be, in this case, the Government agency decides or the procurement officer decides what is needed to be secret and top secret?

Mr. SHENOY. I believe the program office decides what it needs to be and the contracting officer basically passes it down.

Chairman TOM DAVIS. Let me ask you this, all of you, have your organizations had informal discussions with DOD about this, calling attention to the problems and the waste?

Mr. WAGONER. Yes.

Chairman TOM DAVIS. And what has been their response, what we heard today?

Mr. WAGONER. Basically, we are working on the issue. Here is our plan. Here are the things we want to do. But we ask, well, what is the specific timeframe? OK, you are going to put this new system in place. When? What is the specific timeline? And that is where it breaks down.

Chairman TOM DAVIS. I did not want to really embarrass anybody today on the first panel. But if you take a look at the GAO report that came out in 1981 and you hear the responses from the agencies at that point, it was that we are working on it then, too. Sooner or later, you just get tired of them working on it.

Mr. WAGONER. The seats still warm here, Mr. Chairman.

Chairman TOM DAVIS. Yes. OK. [Laughter.]

From the testimonies it is clear that a pseudo black market exists when it comes to employees with security clearances. Can you tell the committee how the dynamics work between large, medium, and small companies? It would seem that the small and medium companies would always lose out to larger companies in these bidding wars or at least have a propensity to lose out. And Mr. Nakamoto, before you testify, I do want to note for the record, I think a positive thing, that we still have GAO and DOD still here. I think they are listening to this. So at least the people we have here today are interested or they would not still be here. The question may be in filtering this up higher. But in this case, talk about the pseudo black markets that exist. I think it is important for these agencies to understand why we end up paying more money for a product, why taxpayers end up paying more money for a product. Gary, if you want to sit at the end, we will get a chair there for you. I think that is a warm seat, too.

Mr. NAKAMOTO. I think one of the things that happens is a smaller company may have fewer employees to spread out their cost. So a larger company may go in and bid, actually just pay the cleared employee a higher rate and spread that over the cost of the contract. So your smaller and medium-size companies will lose out to that employee. But what that means to the taxpayer and the Government overall is what was alluded to earlier in testimony, is that the actual cost escalations for security-type projects continues to grow, and it means that companies that may have open slots on smaller projects remain unfilled. So what you have is an imbalance both in cost escalation and the fact that there are not services being provided to the Government agency.

So I think overall, at the very end of the day, when you weigh these two components out, as well as all the other turmoil that it may cause for a smaller vendor, I think it hurts the business' ability to make money, I think it hurts the Government's ability to have service provided to them, and I think it hurts the taxpayers' investment because they are paying more for a service that they should not have to pay. And when you have a situation where business loses, Government loses, and the taxpayer loses, it is the worst of all worlds.

Chairman TOM DAVIS. Let me understand this. Maybe you hire somebody, your company, a good company but you are not Lock-

heed-Martin. You are a good level, performing well, good small or mid-size company, you hire somebody for $75,000 a year and they have a clearance and they start working on a contract. But there are thousands of other jobs that require people with clearances. And what can happen then, as I understand it, is one of these other companies will come in, they need somebody with a clearance, they go after your guy and they can pay him more.

Mr. NAKAMOTO. That is right.

Chairman TOM DAVIS. And then you cannot complete your aspect of the contract, or you get in a bidding war for somebody that is worth something, but the clearance is what makes it worthwhile. It ends up costing money, contracts do not get completed on time, and the work product suffers. Is that fair?

Mr. NAKAMOTO. Yes, it is. And the other dilemma is, for instance, touching on the one situation where someone will get an interim clearance at one agency and be able to perform an appropriate level of work, and then another agency will make that employee wait even though they have an interim clearance and there is work that they could perform, they are still sitting on the bench. And I would say that it affects all levels of business—large, small, and medium. So I think the situation is deep and it is widespread. I really do believe that it does begin with the manpower situation, human power, but I also believe that it is going to take the Government to recognize the problem and act.

Chairman TOM DAVIS. I had the CEO of Northrop Grumman in my office yesterday just saying the same thing. They probably have an advantage in bidding over you, but they cannot get the people either. So you have these contracts just drying on the vine. The Government needs the service now. They cannot get it now. And what they are getting they are overpaying for.

Ms. Kilberg.

Ms. KILBERG. Mr. Chairman, we talked before about much of the cutting-edge technology coming from small- and mid-size companies, most of our companies of that size cannot afford to put people just on the bench in a hold while they are waiting for their clearances, where the large companies can if they have to.

The other thing is, in our survey, nearly 70 percent of the respondents recruit only cleared workers from Government or other contractors—70 percent. So that tells the story right there.

Chairman TOM DAVIS. So what do you do if you want to get in the business, you are a smart person, you do not have a clearance? It is hard to get a clearance if you do not have a contract lined up.

Ms. KILBERG. You cannot.

Chairman TOM DAVIS. You cannot just go up and say, you know, I have just graduated from college, I want to get a security clearance. It does not work that way.

Ms. KILBERG. That is the chicken and egg, that is your catch–22.

Mr. SHENOY. That is where the problem comes in. A small company cannot afford to have a bench.

Chairman TOM DAVIS. Because you have to carry them in the meantime and you cannot bill them.

Mr. SHENOY. You have to carry them. And every time we have one person on the bench, the cost to the Government for that per-

son goes up by almost 8 percent for every month for that first year. Basically, his cost goes into overheads.

Chairman TOM DAVIS. I guess the way I would understand it, it is kind of like Albert Bell getting $11 million sitting on the bench last year for the Orioles. You just cannot afford to do that.

Mr. SHENOY. Yes. Something like that. [Laughter.]

Chairman TOM DAVIS. I am just trying to put it in terms, you understand. Mr. Schrock and then Mr. Moran.

Mr. SCHROCK. Thank you, Mr. Chairman. I think everything has pretty much been said. I really appreciate all of your coming here today. It sounds to me like standardized clearances might be, Gary, what you just said, standardized clearances would probably help this situation. I guess it is because there are not enough people to do the clearances and that is why it takes so long; is that the basic problem, Bobbie?

Ms. KILBERG. Well, it is partially that you do not have enough people doing the clearances, and it is also partially that you are reinventing the wheel every time. Your example of the young employee who came out of the military, that is not unusual. That is normal for the course.

Mr. WAGONER. And if I may, sir. I think Bobbie brought up a good point, which is that the folks here are dealing with policy that was written probably in the Eisenhower administration on how to do these clearances. And you take a look at data mining, how much can we just off-load, at least do triage on some of these cases and so if the person has bad credit, they have a criminal conviction, have the data mining find that first and get them out of the system.

Mr. SCHROCK. We heard the last panel talk about studies. How do you account for all the studies? What are they studying? I mean, it seems pretty cut and dry. There is a problem, we know what it is, we need to get it fixed. What are they studying?

Ms. KILBERG. I think they are studying the inevitability of giving up their own bureaucratic turf in different agencies and departments.

Mr. SCHROCK. Bingo.

Ms. KILBERG. But then I am not very politically correct usually.

Mr. SCHROCK. Well I am not either, so that is fine. That is why you and I have always gotten along.

That is all I have to say, Mr. Chairman.

Chairman TOM DAVIS. OK. Mr. Moran.

Mr. MORAN. Thank you, Mr. Chairman. I think Ms. Kilberg answered it quite accurately. This is in large part a matter of turf and trust, particularly with regard to reciprocity. There are just so many things that seem inexplicable here. Why, when somebody has just gotten out of the military or some other position where we know they have already been screened, why you cannot facilitate the process of review, why you have to go all the way back. And then, even worse, when another Government agency has already gone through the process but yet the new agency will not accept the work that they have done. Talk about inefficiency and waste. Of course, the worst waste is the end result, where we are paying so much more for people and where our ability to fight wars, to provide needed services and technology to troops in the field and

to make this country's citizens more secure is not being accomplished because we have gotten ourselves inundated in this mountain of paperwork, much of it unnecessary.

Now it was mentioned, I think you just mentioned it, Mr. Wagoner, about the technology that is available. Why you cannot do an initial screening, we have all that information available, we do it for other purposes currently—DOT, in intelligence—we are doing it, we have the software, you can immediately kick out people that have criminal convictions, people that have associations with organizations or individuals that are suspect. You can immediately kick those people out. What you are then left with is a group that should probably be given the benefit of the doubt but at least you should be able to facilitate an investigation of those. And yet, we are not doing it. What we are doing for 6 months, actually, it is 375 days, so for a full year to spin wheels, reinventing the wheel is just beyond us.

I guess I want to ask witnesses here, before this became such a problem, did you have any people that you found compromised your mission, your operations, your ability to meet the Government specifications and requirements?

Mr. WAGONER. If I may. One point I do not think we have talked about is most of our members do our own pre-screening even before, and it is another cost that we have not talked about, because we do not want to take the time and the money to send somebody that we know is going to be rejected. Almost every single one of our companies does at least a credit and a criminal conviction check that we pay for, and many more even do a drug check as well. And then on top of that, to answer your question, from what we understand, the rejection rate is less than 1 percent. So there is not a lot of cases being rejected here.

Mr. MORAN. So, and that is really the bottom line, how likely is it that we are going to find any problems when the corporations have already done the screening. And it would be insane for you to take chances with anybody that you thought might be a security risk, because not only does it jeopardize that contract, it jeopardizes your credibility in being able to go after other contracts. So you are going to do everything possible to screen the people you are hiring anyway. And so now we go through this overlay of more and more investigations, lack of reciprocity, and what seems to be an unjustifiable bureaucratic delay.

I think the chairman has identified something that is in desperate need of correction. And if you have some suggestions, we can put some language in defense appropriations. You hate to have to do that. You wish that the executive branch would fix their own problem. But it looks like it is time to mandate that it be fixed with timeframes and providing whatever resources are necessary, even though I know DOD is going to say we do not need any more money. But if you want to work with us on some language that would go through Chairman Davis so that it would be consistent with what the authorizing committee wanted to see, I am confident that the Defense Appropriations Committee would be happy to put it in that and/or the defense authorizing committee.

Mr. WAGONER. We would be happy to do that. And we already have, as I mentioned in my testimony, our White Paper is already

signed by nine other organizations and so we will work with that coalition we already have together to take you up on the opportunity, and we appreciate that.

Mr. SHENOY. I just wanted to make a comment on what Mr. Wagoner just said. Many companies do their background research but most small companies do not go through that process. It is prohibitively expensive for smaller companies to do. So we will not try to second guess what goes on in the investigative process; however, we do feel it is necessary that the investigations are to be thorough and properly done. The kind of investigations that we as companies do is probably not adequate. I just want to throw that in there.

Mr. MORAN. But you and Mr. Nakamoto, for example, would be looking at an employee pool that in some ways would have been pre-screened. I mean, you are not looking at groups of people to hire that would be likely security risks.

Mr. SHENOY. Absolutely. But there is another problem here. Even when we hire people with top secret clearance from another company, it still takes between 2 to 4 weeks to have that person start on the project simply because there is a process that you are to go through on each task order. It is not like we can pick up the phone, call the contracting office and say, OK, I have hired a top secret guy and we are going to start him on the project. That does not happen.

Mr. MORAN. If you can give us some suggested wording, maybe we can do that, if it meets with the approval of the chairman of this committee.

Mr. SHENOY. Thank you.

Chairman TOM DAVIS. I think one of the things we can do is start by codifying, maybe closing some loop holes in the Executive order on reciprocity and moving some of that. And then you have the manpower, I guess, more appropriately, I would call it the dedicated human capital resources that are needed in this as well. Those are some things that we will try to address.

In the meantime, I just hope that OPM and DOD will continue to meet with industry and look at ways that on their own, without congressional intervention, they can move this along. It is a serious, serious problem that every day makes our country less safe and costs taxpayers unneeded billions of dollars.

We appreciate your being here to set the record straight from your perspective and to lend what I think are some very fruitful ideas in terms of how we may be able to correct this over the short term. The long term, who knows, it has been since 1981. So we need to do some things immediately that can move this backlog. Thank you all for being here today.

The meeting is adjourned.

[Whereupon, at 12:25 p.m., the committee was adjourned, to reconvene at the call of the Chair.]

[Additional information submitted for the hearing record follows:]

PERSEREC

Technical Report 04-2
April 2004

Reciprocity: A Progress Report

Katherine L. Herbig
Northrop Grumman Mission Systems

Peter R. Nelson
Northrop Grumman Mission Systems Consultant

Research Supported by
Personnel Security Managers' Research Program

Research Conducted by
Defense Personnel Security Research Center

Approved for Public Distribution:
Distribution Unlimited.

Executive Summary

Introduction

Reciprocity is a policy that requires acceptance of equivalent personnel security clearances and accesses across the executive branch of the federal government. Authority for the current reciprocity policy is found in an executive order issued in 1995 by President William J. Clinton: Executive Order (E.O.) 12968, *Access to Classified Information*. Two years later the President approved uniform guidelines, mandated in the executive order, in the *Adjudicative Guidelines and Investigative Standards*. They have been implemented throughout the executive branch. The Personnel Security Managers' Research Group (PSMRP) tasked the Defense Personnel Security Research Center (PERSEREC) in 2002 to conduct research on reciprocity that would evaluate the policy and identify potential options for action.

Background

A thorough literature review was undertaken in relevant government policy documents, studies, audits, and working group reports to document the history of the current reciprocity policy. This section traces the evolution, particularly in the Department of Defense (DoD), from localized to more consolidated functions in the three activities that define personnel security: background investigation, adjudication, and maintenance of accurate records on the current status of an individual's accesses. It also describes the development of the reciprocity policy itself. We argue that until the basis for a certain level of standardization was achieved, through advances such as the Single Scope Background Investigation (SSBI), partial consolidation of adjudication within DoD in 1993, and the increasing reliance on electronic databases for records maintenance, reciprocity across the various agencies and military departments of the executive branch could not be expected. With these and other milestones in place by 1995, the long-discussed policy of reciprocity was mandated in E.O. 12968.

Approach

In order to gather information with which to evaluate reciprocity, we conducted interviews with security directors and their staff members at 14 government agencies and five defense contractor companies. Semi-structured interviews were used based on a protocol developed to explore the major issues of reciprocity. During the interviews, informants were encouraged to expand on issues as appropriate and to apply questions to the particular circumstances and needs of their agencies. This produced narrative data that was organized by topic. By speaking with a wide variety of individuals who were conversant with the workings and failings of reciprocity, we learned that some aspects of the policy are working out better than others.

Findings

According to interview respondents, among the interactions in which reciprocity has been improved and now works quite well were visits between agencies, the community badge, and routine updating of the form that initiates a background investigation, the "Questionnaire for

National Security Positions," also known as the SF-86, or in electronic form as the "Electronic Personnel Security Questionnaire," the EPSQ. Visit request and access certification systems are widely familiar, and people look forward to further efficiencies from the networking of electronic databases. The community badge has improved visit reciprocity within the 13 agencies of the Intelligence Community (IC) because typically it is recognized across agencies without the need to pass certifications for each visit. Most agencies reported that they routinely require an updated SF-86 from applicants for access longer than a visit. Under current policy, agencies are responsible to assure themselves that no security-relevant issues have appeared in applicants' lives since their most recent background investigation. Thus it is widely accepted that requiring an updated form since the previous background investigation is prudent and necessary. This allows an agency to do further investigation if security-relevant issues emerge. However, procedures for updating this form are hardly standardized across agencies, and updating currently takes time and causes delays that the framers of reciprocity policy sought to avoid. Respondents hoped that adoption of the SF-86C form, which allows an annual electronic update of one's SF-86 on file in order to keep the information current, would improve the efficiency of what they saw as a necessary procedure.

From the interviews it seemed that certain procedures that require reciprocity have improved since E.O. 12968 but still fall short of actual reciprocity. Three of these areas were: initiatives to expand the use of electronic databases; the review of the files of prior background investigations; and the reciprocal acceptance of the results of polygraph tests.

Respondents strongly agreed that reciprocity depends on access to up-to-date and accurate information about the following: the current status of an individual's clearances and accesses, type and date of background investigations, and an explanation of exceptions, issues, and the adjudicative reasoning that was followed. They also agreed that although this ideal does not yet exist, progress was being made toward it. The networking being done to link or exchange some types of records between various databases being developed was eagerly awaited by most respondents. Many expected that DoD's Joint Personnel Adjudication System (JPAS), which will document adjudication decisions made across DoD agencies and departments, would facilitate reciprocity by offering timely and convenient access to these data for agencies across the government checking on a person's clearance status. The recent creation of data links between JPAS and the Clearance Verification System (CVS), which has been developed by the Office of Personnel Management (OPM), further enhances the ability to quickly check a person's status in an electronic file. The more convenient and accurate these tools for records maintenance and verification become, the more they will contribute to reciprocity.

Although reciprocity policy discourages redundant investigation and re-adjudication, more than half of respondents among executive agencies said they routinely request prior background investigations for review. The reasons given for these reviews clustered around several related concerns. Respondents typically assumed that the particular demands of their own agencies required extra caution. Some felt that because these demands were above and beyond the norm, prudence dictated a review of the investigative file in order to meet their agency's security responsibilities. There was general awareness that policy and regulations do not allow re-adjudication of a past investigation without good reason, that is, unless new security-relevant issues have arisen since the last adjudication. However, for most respondents, the need to check

for new issues since the last investigation justified reviewing recent investigative files. This step of requesting and reviewing files of previous investigations added several weeks or even months to the process of personnel transferring between agencies, and it was this type of delay that the framers of reciprocity policy sought to mitigate.

There are differences of opinion among executive branch agencies about the reliability of polygraph testing, and these differences prevent mandating reciprocity of polygraph testing across all federal agencies. Instead, agencies in the IC that do incorporate the polygraph into their security procedures work reciprocally with one another based on a Memorandum of Agreement (MOA) that was reached in 1998. Information from respondents suggested that IC agencies were often willing to accept a favorable polygraph from another IC agency—and not to insist that the applicant take another test—but that this acceptance depended on which agency had performed the test, the scope of the test, and how recently it had been taken. IC agencies vary among themselves about the scope and recency of previous polygraph testing they require before they demand that an individual take another test given by their own agency.

Several common procedures in personnel security serve to put people to work more quickly, but these procedures also pose problems for reciprocity policy. Interim security clearances and accesses are issued by many agencies while normal background investigation and adjudication procedures are still underway, as long as initial records checks support this shortcut. E.O. 12968 recognizes interim accesses but it mandates that only the agency issuing an interim needs to recognize it. The implication is that if an agency is willing to take a risk on an individual by granting access before all clearance procedures are complete, that agency alone should bear the risk. Others are not required to join into it based on a judgment that they did not make. Over the past several years agencies have been issuing more interim clearances in an effort to have people working while they wait for their final clearance decisions. This became more apparent when a backlog of investigations built up in DoD in the late 1990s that delayed the completion of thousands of investigations, while the attacks of September 11, 2001, created an urgent demand for specialized language and analytic skills. Persons with interim clearances can rarely move reciprocally to other agencies, and typically if they do move, a new background investigation is initiated. Similarly, regulations allow agencies to grant an individual a waiver of adjudicative standards, but exceptions that make sense to one agency may not seem reasonable to another. Waivers, like interims, affect the policy of reciprocity by increasing the inconsistencies practiced across what are supposed to be uniform standards.

There are some aspects of reciprocity that currently appear not to work well. These include conversion of responsibility for accesses from one agency to another, reciprocity for industrial contractors and among Special Access Programs (SAPs), and a basic distinction among agencies between suitability and security that challenges assumptions in reciprocity policy.

The authorizing agency that grants a security clearance or access continues to exercise responsibility for its decision as long as the individual works with information in its care. For access to Sensitive Compartmented Information (SCI), only a specified group of Senior Officials of the Intelligence Community (SOICs) and their designees (defined in E.O. 12333 issued in 1981) hold the authority to grant SCI access from the Director of Central Intelligence (DCI) and,

in the executive orders ultimately by the President. Keeping track of the proper authority over a clearance when a person moves from one agency to another, the type and dates of previous background investigations he or she has undergone, and the start and end dates of a conversion challenge the existing record-keeping systems. Too many times information must be tracked down, delaying moves and adding paperwork. Differences among agencies in their procedures for initiating, tracking, and verifying conversions weaken reciprocity.

Reciprocity is one of the main goals of the National Industrial Security Program (NISP), which has oversight over personnel security for industrial contractors. The NISP includes a structure of authority divided between four co-equal Cognizant Security Agencies (CSAs), and this can challenge reciprocity. The goal of treating the many thousands of industrial contractors reciprocally with government employees runs into difficulty because it downplays an underlying difference: by definition, contractors perform specified tasks or services for a fee, while government employees are entrusted with upholding the government's interests, including its control over its sensitive information, on behalf of the nation. Contractors we interviewed noted that when contractor employees with eligibility access could not move from working on a contract sponsored by one agency to a contract sponsored by another, these failures of reciprocity continue to cost money, time, and talented potential employees who give up and move on.

Lack of reciprocity between SAPs of like protection levels was a particular problem for industry respondents, who often work for many of these programs at once. Reciprocity among SAPs is explicitly mandated in E.O. 12968, yet the several large defense industry contractors interviewed agreed that for their companies, reciprocity among collateral clearances and reciprocity among SCI accesses each worked more smoothly than it does with SAPs. SAPS seemed to respondents to resist reciprocity, and this entailed extra cost and effort for them. Numerous respondents pointed to SAPs as reluctant to recognize reciprocity, many resisting reciprocity even for visits. Despite the patient efforts by committees to identify and promote uniform procedures, respondents noted that SAP personnel understand their programs to occupy extraordinary levels of access defined in good part by themselves. Lack of trust in the judgments of others in the face of these rigorous security demands means that SAPs seem unlikely to achieve complete reciprocity.

Finally, E.O. 12968 separates determinations of eligibility for access to classified information from suitability decisions for employment or retention of employees. Decisions on suitability for hiring remain the prerogative of the agency, and reciprocity policy applies only to the decision on eligibility for access to classified information. In practice, however, the perceived security demands of various agencies blur this distinction between suitability and security. Respondents in the IC noted that the particularly sensitive work of their agencies demanded security eligibility as a condition of suitability for employment—the distinctions between suitability and security disappear when covert intelligence and analysis of SCI are the nature of the work. Whether agencies experience security and suitability as separable or inseparable divides them into two camps that are difficult to bridge with reciprocity.

Consequences of Lack of Reciprocity

Respondents agreed on the adverse impact that a lack of reciprocity has on procedures in their agencies or companies: inefficiency, waste of time, waste of money, and loss of talent when applicants cannot wait any longer for jobs or assignments. There was general agreement that improved reciprocity would increase efficiency, lower costs, and thus would benefit the government.

Reasons for Lack of Reciprocity

When asked about the reasons for lack of reciprocity, respondents pointed to two interrelated issues: turf and trust. Many pointed to a determination to exert ownership over the security clearances and accesses held within agencies that reflects the responsibility people feel for the information entrusted to their care. Having adjudicated a decision about an individual and granted access, an agency can feel that the access belongs to it. Virtually all respondents agreed that beneath the lack of complete reciprocity there is a certain lack of trust based on fear. Lack of trust is a symptom of the same structural reality that produces "turf battles." People trust what is familiar and what they can control or at least influence, and they distrust what is less familiar and what they cannot control. Investigations and adjudications done by others, even though they work with the same prescribed standards and guidelines, seem less trustworthy than those done by "our people."

Respondents pointed to various issues with both the performance of background investigations and with adjudication that they felt reduce reciprocity. These included the multiplicity of government and private entities performing background investigations that result in differing procedures and judgments. Agencies vary in the resources they can commit to personnel security: Some agencies have hundreds of thousands of investigations to process each year, others only have hundreds and can afford to perform additional procedures. Respondents pointed to the lack of uniform personnel standards for investigators and for adjudicators, and a lack of common training in both professions, as reasons for inconsistent application of guidelines. These perceived inconsistencies produced a sense that the judgment of others could be untrustworthy.

Some respondents expressed skepticism about the necessity for complete reciprocity that is mandated in E.O. 12968. The advantages of standardized and centralized personnel security procedures—benefits such as reducing costs by eliminating duplication and redundancies while increasing efficiency—can be balanced against potential disadvantages. One disadvantage mentioned is a decoupling of accountability for security from the human judgments made by an agency in its vetting procedures. Thus, reviewing the file of an existing background investigation, and possibly re-investigating and re-adjudicating, are seen as procedures that give a prudent second look by a new set of eyes—a second look that is likely to enhance the quality of the decision and therefore the level of security. To respondents who argued that complete reciprocity should not be the government's goal, the distinctiveness of agencies in the IC was more significant than the presumed benefits of standardization. These would argue that a more nuanced reciprocity, which recognized differences among the communities, should be developed.

Options for Action

1. Continue Doing More of the Same. Some respondents thought it best not to tinker further with the policies, authorities, and procedures affecting reciprocity. Among these, some felt that the current level of reciprocity was all that could be expected, while others felt that on-going work would lead to continued improvements in reciprocity.

2. Try Money. Some respondents felt that a disparity among the various agencies in the funding personnel security programs seriously hinders reciprocity, and that agencies such as DoD, the agency with a large majority of the eligibility accesses, should invest more resources in order to bring its program to a level more like those in the IC.

3. Restructure the Context for Reciprocity. Some respondents expressed frustration with the inability of "some overarching Governmental authority to impose the reciprocity standards in E.O. 12968 on the rest of the government." It has been characteristic of personnel security policy that new initiatives like reciprocity have been overlaid onto existing policies without a complete reworking and integrating of the old and the new. E.O. 12968 was a compromise in 1995 that left in place competing authorities and prerogatives. Possibly the new demands placed on the government by the terrorist attacks in 2001 have diminished the urgency of reciprocity policy for the present, but eventually a restructuring of the authorities that underlie responsibility for national security information will be necessary if reciprocity is to become more complete.

4. Eliminate the Need for Reciprocity by Consolidation. Some suggested that consolidation of personnel security functions is the best approach. Creating a single organization to do background investigations across the federal government, and a single organization to do adjudication, and a single database that would be accessible to anyone checking clearance status would simplify these functions and holds out the promise of consistency, uniformity, and accountability. However, this approach deemphasizes the distinctions among agencies, and differences that flow from them, which many find crucial.

5. Redefine Reciprocity to Reflect Differences between the IC and Other Agencies. Some argued that there are irreducible distinctions between the IC and non-IC agencies. While in this view reciprocity among IC agencies profitably could be developed further, reciprocity between the IC and non-IC agencies should be redefined to acknowledge these distinctions. From this perspective, complete reciprocity should not be the goal of the federal government and a policy with more gradations should be developed.

EO 12968 here are the applicable parts dealing with portability and standardization:

Note that the underlined parts allow the agency to refuse reciprocity under certain conditions . . . .

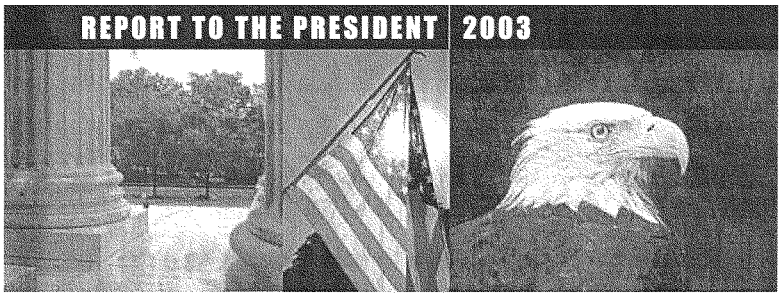
Sec. 2.4. *Reciprocal Acceptance of Access Eligibility Determinations.* (a) Except when an agency has substantial information indicating that an employee may not satisfy the standards in section 3.1 of this order, background investi-gations and eligibility determinations conducted under this order shall be mutually and reciprocally accepted by all agencies.
(b) Except where there is substantial information indicating that the employee may not satisfy the standards in section 3.1 of this order, an employee with existing access to a special access program shall not be denied eligibility for access to another special access program at the same sensitivity level as determined personally by the agency head or deputy agency head, or have an existing access eligibility readjudicated, so long as the employee has a need for access to the information involved.
(c) This section shall not preclude agency heads from establishing additional, but not duplicative, investigative or adjudicative procedures for a special access program or for candidates for detail or assignment to their agencies, where such procedures are required in exceptional circumstances to protect the national security.

According to these sections, it looks like the Security Policy Board is responsible for setting up standards and for guiding agencies toward cooperation.

Sec. 3.1. (f) Not later than 180 days after the effective date of this order, the Security Policy Board shall develop a common set of adjudicative guidelines for determining eligibility for access to classified information, including access to special access programs.

Sec. 3.2. (b) Not later than 180 days after the effective date of this order, the Security Policy Board shall develop a common set of investigative standards for background investigations for access to classified information. These standards may vary for the various levels of access.

Sec. 6.1. *Agency Implementing Responsibilities.* Heads of agencies that grant employees access to classified information shall: . . .
(b) cooperate, under the guidance of the Security Policy Board, with other agencies to achieve practical, consistent, and effective adjudicative training and guidelines; . . . .



INFORMATION SECURITY OVERSIGHT OFFICE

March 31, 2004
The President
The White House
Washington, DC 20500

Dear Mr. President:

We are pleased to submit to you the Information Security Oversight Office's (ISOO) 2003 Report.

This Report provides information on the status of the security classification program as required by Executive Order 12958, "Classified National Security Information." It includes statistics and analysis concerning components of the system, primarily classification and declassification. It also contains information with respect to the implementation of industrial security in the private sector as required by Executive Order 12829, "National Industrial Security Program."

The hallmark of 2003 was, of course, the amendment you issued to Executive Order 12958. In this revision, you called upon all agencies to make the concept of automatic declassification of 25 year-old or older historical classified records a reality by December 31, 2006. Other changes reflected eight years of experience in implementing the Order, as well as new priorities resulting from the events of September 11, 2001. In September 2003, ISOO issued the directive implementing the revised Executive Order. We will be working on continued refinements to the security classification system in order to make it more conducive to the electronic environment in which agencies increasingly operate.

As noted in this Report, implementation of the National Industrial Security Program seems to be at a crossroads. Several issues, including excessive security clearance delays for industry, continue to hamper industry's ability to be responsive to Government's needs The responsible agencies have developed a number of initiatives addressing this long standing issue on security clearances, as well as other issues.

Ultimately, the full implementation of the security classification system and the industrial security program is designed to equally promote an informed and protected American public. Deliberate, continuous effort is required to succeed at both—the American people expect and deserve nothing less.

Respectfully,

J. William Leonard

Director

INFORMATION SECURITY OVERSIGHT OFFICE

AUTHORITY

Executive Order 12958, as amended, "Classified National Security Information," and Executive Order 12829, as amended, "National Industrial Security Program." The Information Security Oversight Office (ISOO) is a component of the National Archives and Records Administration and receives its policy and program guidance from the National Security Council (NSC).

MISSION

ISOO oversees the security classification programs in both Government and industry and reports to the President annually on their status.

FUNCTIONS

★ Develops implementing directives and instructions.

★ Maintains liaison with agency counterparts and conducts on-site inspections and special document reviews to monitor agency compliance.

★ Develops and disseminates security education materials for Government and industry; monitors security education and training programs.

★ Receives and takes action on complaints, appeals, and suggestions.

★ Collects and analyzes relevant statistical data and, along with other information, reports them annually to the President.

★ Serves as spokesperson to Congress, the media, special interest groups, professional organizations, and the public.

★ Conducts special studies on identified or potential problem areas and develops remedial approaches for program improvement.

★ Recommends policy changes to the President through the NSC.

★ Provides program and administrative support for the Interagency Security Classification Appeals Panel (ISCAP).

GOALS

★ Promote and enhance the system that protects the national security information that safeguards the American Government and its people.

★ Provide for an informed American public by ensuring that the minimum information necessary to the interest of national security is classified and that information is declassified as soon as it no longer requires protection.

★ Promote and enhance concepts that facilitate the sharing of information in the fulfillment of mission-critical functions related to national security.

TABLE OF CONTENTS

Summary of Fiscal Year 2003 Program Activity 4

The Importance of Basics 5

Interagency Security Classification Appeals Panel 7

National Industrial Security Program 10

Classification 11

Declassification 20

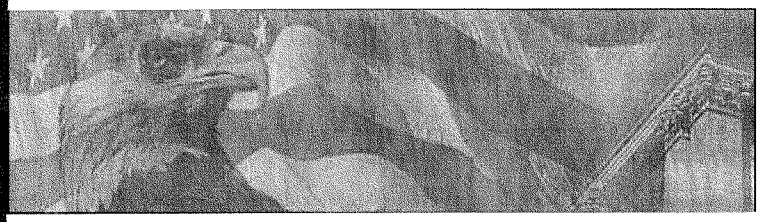
Agency Acronyms and Abbreviations 28

ISOO Classified National Security Information Directive No. 1 .....Back Pocket

Note: The Report on Cost Estimates for Security Classification Activities will be reported separately.

SUMMARY OF FY 2003 PROGRAM ACTIVITY

The following Report to the President is the eighth report under E.O. 12958, which went into effect in October 1995, and was amended on March 25, 2003. The following data highlight ISOO's findings.



Classification

★ Executive branch agencies reported 3,978 original classification authorities.

★ Agencies reported 234,052 original classification decisions.

★ Executive branch agencies reported 13,993,968 derivative classification decisions.

★ Agencies reported 14,228,020 combined classification decisions.

Declassification

★ Under Automatic and Systematic Review Declassification programs, agencies declassified 43,093,233 pages of historically valuable records.

★ Agencies received 5,354 new mandatory review requests.

★ Under mandatory review, agencies declassified in full 218,764 pages; declassified in part 80,520 pages; and retained classification in full on 10,889 pages.

★ Agencies received 43 new mandatory review appeals.

★ On appeal, agencies declassified in whole or in part 1,465 additional pages.

THE IMPORTANCE OF BASICS

Fiscal year 2003 saw significant activity with respect to the framework employed to classify national security information. Yet, even with the signing on March 25, 2003, of Executive Order 13292, further amending Executive Order 12958 on classified national security information, what is most notable about the new amendment is what did not change with respect to the fundamentals that make the security classification system work.

To bring to bear the capabilities of the classification system for national security information, the information's originator need simply affix certain classification markings. However, it is not the security markings on the media that protect truly sensitive information from unauthorized disclosure; rather, it is the people who deal with the information, their knowledge and understanding of the program, and their belief in the integrity of the system represented by the markings. This knowledge, understanding, and confidence cannot be taken for granted.

The security classification system is no different than other systems in that it requires continuous attention and upkeep. Left alone, the system will likely corrode and lose its overall effectiveness, placing in jeopardy all information cloaked in its protective measures. This, of course, has more than theoretical consequences in time of war; especially with respect to the resulting damage to the common defense should such information be subject to unauthorized disclosure. Yet, if we are not attentive, the demands of war can distract us from doing what is necessary today to ensure the continued efficacy of the security classification system. The security classification system is not self-directing—it works only when leadership demonstrates personal commitment and directs senior management to make it work.

Executive Order 12958, as amended, is replete with measures to ensure the classification system's continued effectiveness. Agencies must appoint senior officials to oversee the agency's program, promulgate internal regulations, establish and maintain security education and training programs as well as an ongoing self-inspection program, and commit the resources necessary to ensure effective implementation of the program, among other requirements. Many agencies are excelling at fulfilling these requirements. According to agency reviews as well as agency submissions in preparation of this report, others are not. In the final analysis, this is a fundamental issue for agency heads and their leadership teams.

Many senior officials will candidly acknowledge that the government classifies too much information, although oftentimes the observation is made with respect to the activities of agencies other than their own. The potential issue of excessive classification is supported, in part, by agency input indicating that overall classification activity is up over the past several years. Yet, some individual agencies are not certain. They have no real idea how much of the information they generate is classified; whether the overall quantity is increasing or decreasing; what the explanations are for such changes; which elements within their organizations are most responsible for the changes; and, most important, whether the changes are appropriate, i.e., whether too much or too little information is being classified and whether it is for too long or too short a period of time. The absence of such rudimentary baseline information makes it difficult for agencies to ascertain the effectiveness of their classification efforts.

Similarly, one of the principal procedures for maintaining the effectiveness of the classification system is to remove from the safeguarding system information that no longer requires protection in the interest of national security. In addition to processes such as automatic and systematic declassification, as well as mandatory declassification reviews, the Executive order clearly states that "information shall be

declassified as soon as it no longer meets the standards for classification" (Section 3.1). Elsewhere, the Order specifically prohibits the use of classification "to prevent or delay the release of information that does not require protection in the interest of the national security" (Section 1.7 (a) (4)). Nonetheless, as noted in this report, declassification activity has been down for the past several years.

In some quarters, when it comes to classification in times of national security challenges, when available resources are distracted elsewhere, the approach toward classification can be to "err on the side of caution" by classifying and delaying declassification "when in doubt" and by "asking questions later." Yet, the classification system is too important, and the consequences resulting from improper implementation too severe, to allow "error" to be a part of any implementation strategy. Error from either perspective, both too little and too much classification, is not an option. Too much classification unnecessarily impedes effective information sharing. Too little classification subjects our nation to potential harm.

Proactive oversight by an agency of its security classification program is not a luxury. Similarly, declassification cannot be regarded as a "fair weather project," something we tend to when resources are plentiful but that quickly falls off the priority list when times get tough, especially in times of national security challenges. Allowing information that will not cause damage to national security to remain in the classification system, or to enter the system in the first instance, places all classified information at needless increased risk.

In response to this concern, ISOO has asked all agency heads to closely examine efforts to implement and maintain the security classification system at their agencies. Each has been asked to give special emphasis to reviewing how they provide their personnel who deal with classified information with the knowledge and understanding required to make the program work, and what positive steps they can take to ensure the continued integrity of the system. This effort includes ensuring that information that requires protection is properly identified and safeguarded and, equally important, that information not eligible for inclusion in the classification system remains unclassified or is promptly declassified. Further, in the interests of information sharing, agencies with original classification authority need to recognize the inherent discretion they have in making such a decision; just because information can be classified does not mean that it should be classified. Finally, the classification framework itself, in the overall context of information sharing and protection at all levels, can benefit from a fresh assessment of how it can be enhanced to better meet the needs of the electronic environment in which the Government increasingly operates. During the coming year, ISOO will be working closely with agencies to ensure that these and other steps are being taken to ensure the classification system's continued effectiveness.

In addition, for the next several years, future editions of this report will emphasize agency progress in fulfilling the direction set forth in the Order to achieve complete implementation of automatic declassification by December 31, 2006. It is essential that agencies recapture the momentum of prior years in their declassification efforts. Special emphasis will be placed on interagency process improvements, especially in the areas of joint training, increased empowerment of reviewers, and increased delegation of authority between agencies.

Our security classification framework recognizes that our democratic principles require that the American people be informed of the activities of their Government and that our nation's progress depends upon the free flow of information. Nevertheless, it also recognizes that throughout our history, the national defense has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations. This is not an either/or challenge. Deliberate, continuous effort is required to succeed at both—the American people expect and deserve nothing less.

INTERAGENCY SECURITY CLASSIFICATION APPEALS PANEL

AUTHORITY

Section 5.3 of Executive Order 12958, as amended, "Classified National Security Information."

FUNCTIONS

(1) To decide on appeals by authorized persons who have filed classification challenges under Section 1.8 of E.O. 12958, as amended.

(2) To approve, deny, or amend agency exemptions from automatic declassification as provided in Section 3.3 of E.O. 12958, as amended.

(3) To decide on appeals by persons or entities who have filed requests for mandatory declassification review under Section 3.5 of E.O. 12958, as amended.

MEMBERS*

William H. Leary, *Chair*
National Security Council

James A. Baker
Department of Justice

Edmund Cohen
Central Intelligence Agency

Margaret P. Grafeld
Department of State

Carol A. Haave
Department of Defense

Michael J. Kurtz
National Archives and Records Administration

EXECUTIVE SECRETARY

J. William Leonard, *Director*
Information Security Oversight Office

SUPPORT STAFF

Information Security Oversight Office

*The individuals named in this section were those in such positions as of the end of FY 2003.

SUMMARY OF ACTIVITY

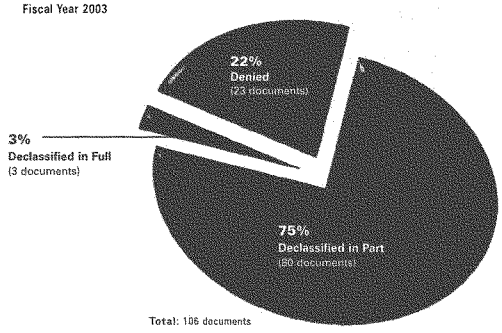
The Interagency Security Classification Appeals Panel (ISCAP) was created under E.O. 12958 to perform the critical functions noted above. The ISCAP, comprised of senior level representatives appointed by the Secretaries of State and Defense, the Attorney General, the Director of Central Intelligence (DCI), the Archivist of the United States, and the Assistant to the President for National Security Affairs, began meeting in May 1996. The President selects its Chair, the Director of the Information Security Oversight Office (ISOO) serves as its Executive Secretary, and ISOO provides its staff support.

To date, the majority of the ISCAP's efforts have focused on mandatory declassification review appeals. During fiscal year 2003, the ISCAP decided upon 106 documents that remained fully or partially classified upon the completion of agency processing.

It declassified the entirety of the remaining classified information in 3 documents (3 percent), and declassified some portions while affirming the classification of other portions in 80 of the documents (75 percent). The ISCAP fully affirmed the agency decisions in their entirety for 23 documents (22 percent).

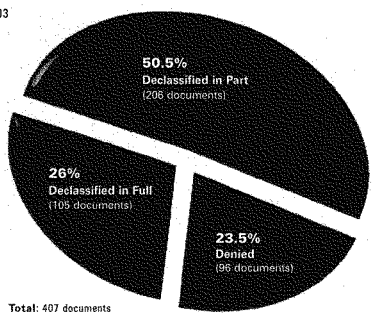
ISCAP DECISIONS

Fiscal Year 2003



From May 1996 through September 2003, the ISCAP has decided upon a total of 407 documents. Of these, the ISCAP declassified information in 76.5 percent of the documents. Specifically, it has declassified the entirety of the remaining classified information in 105 documents (26 percent), and has declassified some portions while affirming the classification of other portions in 206 documents (50.5 percent).

ISCAP DECISIONS
May 1996 – September 2003



Total: 407 documents

The ISCAP has fully affirmed agency classification decisions in 96 documents (23.5 percent). Documents declassified by the ISCAP may be requested from the entity that has custody of them, usually a presidential library. For assistance in identifying and requesting copies of such documents, or for any other questions regarding the ISCAP, please contact the ISCAP staff at ISOO.

During fiscal year 2003, the ISCAP also approved declassification guides submitted by the Department of the Navy and the Joint Chiefs of Staff in accordance with Section 3.3(b) of E.O. 12958, as amended, and the applicable provision of its government-wide implementing directive (32 C.F.R. Part 2001.32(c)). When approved by the ISCAP, such guides authorize the exemption of information determined by an agency head to fall within an exemption category listed in Section 3.3(b) of the amended Order. Essentially, the guides permit certain information to be classified for more than 25 years. In order to gain ISCAP approval, guides must provide a comprehensive description of the information proposed for exemption, a distinct relationship to a specific exemption, a justification or explanation of the need for exemption, and a fixed date or event for future declassification.

If you have any questions concerning the ISCAP, please contact the ISCAP staff :

202.219.5250 

202.219.5385 

iscap@nara.gov

www.archives.gov/isoo/oversight_groups/iscap.html

Amendment to E.O. 12958 regarding the Director of Central Intelligence (DCI)

With the amendment of E.O. 12958 in fiscal year 2003, the DCI has the ability to block ISCAP declassification of certain information owned or controlled by the DCI, requiring that the DCI's determination be appealed to the President (see Section 5.3(f) of the amended Order). ISOO will report annually on the use of this provision.

NATIONAL INDUSTRIAL SECURITY PROGRAM

Through Executive Order 12829, the President formally established the National Industrial Security Program (NISP) on January 6, 1993. The Order calls for a single, integrated, cohesive system for safeguarding classified information held by industry. Consistent with this goal, the four major tenets of the NISP are as follows:

- ★ Achieve uniformity in security procedures.
- ★ Implement the reciprocity principle in security procedures, particularly with regard to facility and personnel clearances.
- ★ Eliminate duplicative or unnecessary requirements.
- ★ Achieve reductions in security costs.

During the early years of the NISP, a substantial amount of positive change was accomplished in a relatively short period. This early success was a direct result of the shared commitment and interest exhibited by top officials within the agencies along with cooperation from key representatives in industry. Recently, however, there is a growing sentiment that the transition to a fully functional NISP is in need of renewed attention by senior management in both Government and industry. Symptomatic of these concerns is mounting frustration over the inability to eliminate the backlog of personnel security clearances, reach true reciprocity in regard to personnel and facility clearances, and accredit industry's automated information systems in a timely manner, despite repeated efforts.

Consistent with ISOO's responsibilities under Section 102(b) of the Order, ISOO began its third survey of the NISP in the summer of 2002. The survey report was finalized in the summer of 2003 and a copy of the report can be accessed at http://www.archives.gov/isoo.

Despite a general acknowledgment that the initial momentum of the NISP has tapered off, there remains a genuine consensus, particularly at the grass roots level, that a revitalized NISP is essential. Although there has been some disagreement as to how the NISP can be revitalized and, in particular, whether ISOO should increase its role within the NISP, the Order outlines several areas where ISOO believes it must increase its role in the implementation and monitoring of the program. These areas will be the focus of our NISP-related activities in the future and will be detailed in future reports.

National Industrial Security Program Policy Advisory Committee

E.O. 12829 established the National Industrial Security Program Policy Advisory Committee (NISPPAC). The Committee, with representation from government and industry, advises the Chairman (ISOO Director) on all matters concerning the NISP. During fiscal year 2003, the NISPPAC met only once. Its 21st meeting was held on April 23, 2003. Of particular note, the Committee voted to add the Department of Homeland Security as a permanent voting member of the NISPPAC. Given the increased role of the Office of Personnel Management (OPM) in personnel security investigations, the Committee also requested that OPM attend future NISPPAC meetings. However, regardless of these changes, slow movement in response to a number of other initiatives caused the Chair to delay the next NISPPAC meeting until fiscal year 2004.

GAO
Accountability * Integrity * Reliability
United States General Accounting Office
Washington, DC 20548

June 25, 2004

The Honorable Tom Davis
Chairman
Committee on Government Reform
House of Representatives

Dear Chairman Davis:

During the May 6, 2004, hearing on security clearances for contractor personnel before the House Committee on Government Reform, you asked me to respond to two questions for the record: (1) What statutorily can this committee do in the short-term to address clearance-related concerns? (2) Should we codify reciprocity of clearances?

Regarding what this committee could do statutorily in the short-term, I believe the committee could initiate legislation that would direct the National Security Council's (NSC) Policy Coordinating Committee on Records Access and Information Security prepare a report that identifies specific requirements for (1) implementing the *Standards for Background Investigations for Access to Classified Information and Adjudicative Guidelines for Determining Eligibility for Access to Classified Information* that were established governmentwide in 1997 and (2) correcting various clearance-related problems that the U.S. General Accounting Office (GAO)—and others—have identified.

Although the 1997 federal investigative standards and adjudicative guidelines have been useful in moving the government toward reciprocity and consistent processes across departments and agencies, differences remain in the implementation of the standards and guidelines. The Department of Defense (DOD), intelligence community, Department of Energy, and other departments and agencies could be required to reach consensus on the minimum conditions that, if met, would result in reciprocal acceptance of a clearance and access. For example, the NSC report could prescribe the number and types of sources needed to satisfy the requirements for conducting interviews as part of the investigative process for determining eligibility for a top secret clearance. Exceptions to reciprocity, the rationale for each exception, and procedures for granting the exception would need to be stated explicitly. The process resulting in the NSC report could provide experts from the various departments and agencies with opportunities to express their concerns about reciprocity as well as concerns about the quality of security clearances (e.g., completeness of the information in investigative reports) and their timeliness (e.g., governmentwide goals detailing how quickly each type of clearance-related investigation should be completed).

Following the issuance of the NSC report, the mandate could include provisions that NSC and its Policy Coordinating Committee on Records Access and Information Security provide GAO with a copy of the report and access to all officials and documents used to produce the report. GAO could then be requested to evaluate the NSC report to determine whether the committee's clearance-related concerns regarding reciprocity, backlogs, timeliness, and quality had been adequately addressed. For example, GAO could assess the adequacy of the NSC report in (1) addressing reciprocity of both clearances and access, (2) prescribing the minimum investigative and adjudicative requirements for the granting of each type of clearance and access, and (3) identifying and recommending solutions to other personnel security clearance-related problems.

This suggestion for addressing reciprocity and other clearance-related issues would supplement eight recommendations that GAO made in its two most recent reports on DOD's personnel security clearance process. DOD concurred or partially concurred with all eight recommendations.

- In our May 2004 report (enclosed) on *DOD Personnel Clearances: Additional Steps Can Be Taken to Reduce Backlogs and Delays in Determining Security Clearance Eligibility for Industry Personnel* (GAO-04-632, May 26, 2004) addressed to you and the Chairman, Subcommittee on National Security, Emerging Threats and International Relations, GAO recommended that the Secretary of Defense direct the Under Secretary of Defense for Intelligence to take the following four actions: (1) improve the projections of industrial personnel clearance requirements, (2) work to eliminate unnecessary reciprocity limitations, (3) develop and implement an overall management plan, and (4) determine the feasibility of implementing promising initiatives.

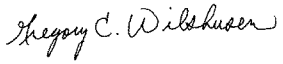
- In our February 2004 report (enclosed) on *DOD Personnel Clearances: DOD Needs to Overcome Impediments to Eliminating Backlog and Determining Its Size* (GAO-04-344, Feb. 9, 2004) to the Ranking Minority Member, House Committee on Armed Services, we recommended that the Secretary of Defense direct the Under Secretary of Defense for Intelligence take the following four actions: (1) match both investigative and adjudicative workforce sizes to workloads, (2) develop a strategic plan to overcome access to information problems, (3) develop DOD-wide backlog definitions and measures and monitor the backlog, and (4) complete the implementation of the automated system for monitoring adjudication-related information.

Regarding whether the Congress should codify reciprocity, GAO has not conducted sufficient work on the reciprocity issue to be in a position to make a recommendation. The scope of our most recent work, for instance, focused on DOD and did not include the intelligence agencies or Department of Energy. The information provided in the NSC report that we suggested earlier in this letter could, however, provide insights into whether reciprocity should be codified. If NSC were to provide this committee with a specific legislative proposal to fully utilize

reciprocity, then GAO would be able to work with the committee in evaluating this—or other—proposals.

If you or your staff have any questions, please contact me at (202) 512-6244 or by e-mail at wilshuseng@gao.gov or contact Jack E. Edwards, Assistant Director, at (202) 512-8246 or by e-mail at edwardsj@gao.gov.

Sincerely yours,



Gregory C. Wilshusen, Acting Director
Defense Capabilities and Management

Enclosures—2

cc: The Honorable Christopher Shays
The Honorable Henry Waxman

Chairman Davis, Ranking Member Waxman, and Members of the House Government Reform Committee,

Thank you for this opportunity to provide written testimony for inclusion in the official Congressional hearing record concerning recommendations to address the current backlog in our security clearance process. I approach this subject from three perspectives: first, as a retired Army officer who spent more than 23 years on active duty; second, as a former Chairman, President & CEO of a publicly-traded IT staffing and solutions company that operated solely in the commercial sector; and third, as the current President and COO of Secure IT Services, the federal division of COMSYS Services LLC, a national IT staffing and services company.

During my time as Chairman, President & CEO of a commercial enterprise my company's main clients were in the financial, insurance and pharmaceutical industries. Beginning in early 2000 and continuing to my departure in October of 2003 I watched the continual erosion of our business as clients outsourced more and more of this work to low cost development centers overseas. More importantly, I witnessed firsthand the human costs associated with having to lay off highly-skilled IT workers - in many cases fairly late in their careers.

I received my MBA from the University of Chicago and have always been an advocate of the free flow of capital and labor, so the call for barriers to outsourcing always struck me as a short sighted "solution" to the problem. I always felt that the real solution was to redeploy this domestic talent to the growing demand coming from the federal government in response to the war on terrorism and in providing the solutions

required for homeland security. So when I was approached by COMSYS with the opportunity to combine my familiarity with how the federal government works with my knowledge of running a large IT staffing and solutions company I saw it as a great opportunity to help meet the critical needs of our government and to help solve a pressing current employment need.

The reason that I am so interested in participating in this forum is that my current experience over the last six months has convinced me that our security clearance process needs to be improved if we are going to be successful in redirecting the available domestic IT talent to the needs of our federal government. I offer you six specific recommendations that I feel would help alleviate the current bottle neck in providing the required IT talent without jeopardizing our valid security requirements.

1. Improve coding: The war on terrorism and the creation of the Department of Homeland Security have created a growing demand for highly-skilled IT workers with security clearances. It is my assessment that many of the jobs that would not have required a security clearance in the past are now being coded as requiring one. While no one would argue that we should jeopardize valid security requirements, the natural tendency of any organization is to err on the side of caution. We should ensure that the benefits of this caution do not exceed the costs associated with the backlog of more than 400,000 security clearances currently in the system. The Information Security Oversight Office (ISOO) should be encouraged to ensure that we don't have "classification" creep as an over-reaction to the current times.

2. Tighten oversight: I am seeing a real increase in what I feel are "vanity clearances" - companies that are placing non-billing resources into the security clearance process solely for the purposes of obtaining a clearance and not because the clearance is actually needed to conduct their day-to-day business with the government. Here again, the ISOO could reduce demand on the system by ensuring that "vanity applications" receive lowest priority in processing.

3. Increase transportability: Wherever possible we should remove the barriers that prohibit transportability of clearances from one agency to another.

4. Increase resources: The Defense Security Service should be given more resources to help cut through the backlog. These resources should include both increased manpower and more efficient and user friendly processes.

5. Build a pipeline: Allow companies that provide secure IT talent to build a project independent pipeline through the issuance of a separate DD 254. A DD 254 is often issued for an entire project and the prime contractor for the government can bring on multiple resources against that DD 254. Why not issue a company like Secure IT Services a DD 254 that isn't associated with winning a piece of work but would be their "license" to build a pipeline of secure resources to apply against future opportunities?

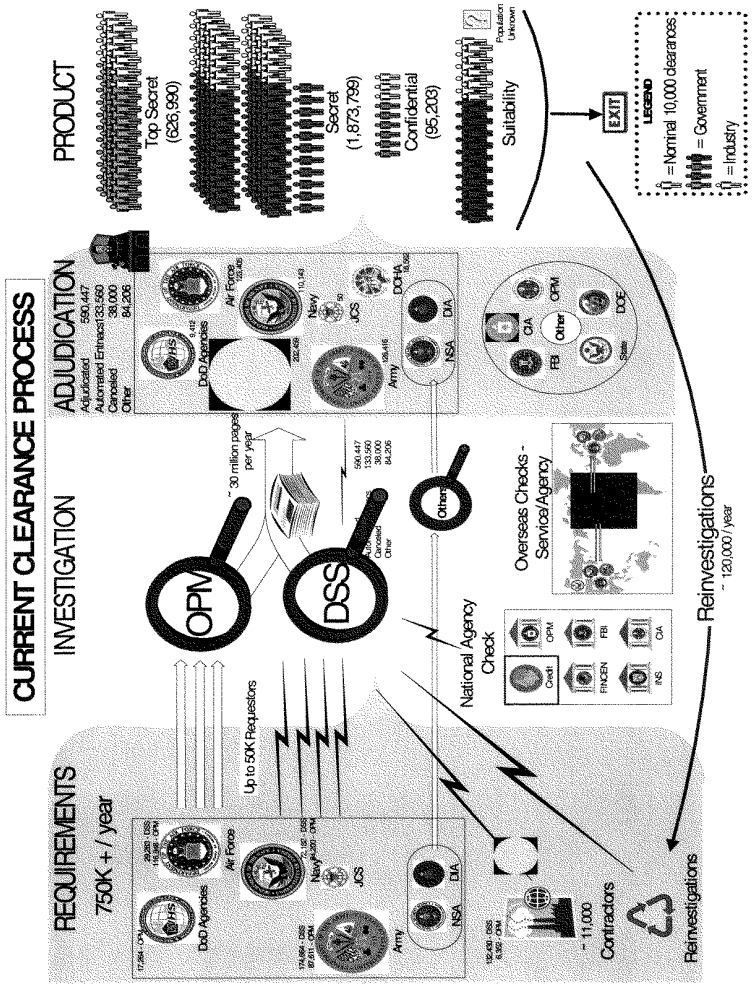
6. Have government sponsor them: Allow individuals to be sponsored by the federal government for their clearances without having to be linked to an individual company's

DD 254. Increase the supply of security cleared IT resources by allowing them to be sponsored for clearance directly by the federal government. Prioritize clearance processing for these individuals based on the needs of the federal government.

I believe these recommendations would have the combined effects of reducing the demand for unnecessary security clearances, increasing the supply of secure IT talent that is available to redeploy from one project to another in a proactive manner, and in improving both the process and the speed of security clearance investigations. Thank you again for this opportunity to participate in this important discussion.

Very Respectfully,

Robert D. Merkl
President and COO
Secure IT Services, a division of COMSYS Services LLC
Rockville, Maryland


CURRENT CLEARANCE PROCESS
REQUIREMENTS
750K + / year
INVESTIGATION
ADJUDICATION
PRODUCT
Top Secret
(626,990)
Secret
(1,873,799)
Confidential
(95,203)
Suitability
Population Unknown
EXIT
LEGEND
= Nominal 10,000 clearances
= Government
= Industry
DoD Agencies
Air Force
Navy
JCS
Army
NSA
DIA
DOHA
~ 11,000
Contractors
Reinvestigations
Up to 50K Requestors
~ 30 million pages per year
OPM
DSS
Other
590,447
133,560
38,000
84,206
National Agency Check
Credit
OPM
FBI
FINCEN
INS
CIA
Overseas Checks - Service/Agency
CIA
FBI
Other
OPM
DOE
State
Reinvestigations
~ 120,000 / year

○