

GAO

Report to the Chairman, Committee on
Government Reform, and Chairman,
Subcommittee on National Security,
Emerging Threats and International
Relations, House of Representatives

May 2004

DOD PERSONNEL CLEARANCES

Additional Steps Can Be Taken to Reduce Backlogs and Delays in Determining Security Clearance Eligibility for Industry Personnel



G A O

Accountability * Integrity * Reliability



Highlights of [GAO-04-632](#), a report to the Chairman, Committee on Government Reform, and Chairman, Subcommittee on National Security, Emerging Threats and International Relations, House of Representatives

Why GAO Did This Study

As more and more federal jobs are privatized, individuals working for private industry 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 must hold a security clearance. As of September 30, 2003, industry workers held more than one-third of all clearances issued by DOD.

Long-standing security clearance backlogs and delays in determining clearance eligibility affect industry personnel, military members, and federal employees. As requested, we reviewed the clearance eligibility process for industry personnel and (1) describe the size of the backlog and changes in the time needed to issue eligibility determinations, (2) identify reasons for the backlog and delays, and (3) evaluate initiatives that DOD could take to eliminate the backlog and decrease the delays.

What GAO Recommends

GAO is recommending that the Secretary of Defense direct the Under Secretary of Defense for Intelligence to improve projections of industry clearances required, eliminate reciprocity limitations, develop an integrated plan to eliminate the backlog and reduce delays, and analyze the feasibility of initiatives to reduce the backlog and delays. DOD fully concurred with three recommendations and partially concurred with one.

www.gao.gov/cgi-bin/getrpt?GAO-04-632.

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

DOD PERSONNEL CLEARANCES

Additional Steps Can Be Taken to Reduce Backlogs and Delays in Determining Security Clearance Eligibility for Industry Personnel

What GAO Found

As of March 31, 2004, DOD's security clearance backlog for industry personnel was roughly 188,000 cases, and the time needed to conduct an investigation and determine eligibility for a clearance during the last 3 fiscal years had increased by 56 days to a total of 375 days. DOD identified three separate backlog estimates:

- more than 61,000 reinvestigations (required for renewing clearances) that were overdue but had not been submitted,
- over 101,000 new investigations or reinvestigations that had not been completed within DOD's established time frames, and
- over 25,000 adjudications (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 conduct an investigation and determine clearance eligibility for industry personnel increased from 319 days to 375 days. Delays in conducting investigations and determining clearance eligibility can increase national security risks, 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.

Several impediments hinder DOD's ability to eliminate the backlogs and reduce the amount of time needed to conduct an investigation and determine security 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 insufficient investigative and adjudicative workforces to handle the large 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. Also, the effects of past conditions, such as the backlog itself, have been identified as impediments to timely eligibility determinations. Furthermore, DOD does not have an integrated, comprehensive management plan for addressing the backlog and delays.

DOD is considering several initiatives that might reduce security clearance backlogs and processing times for determining clearance eligibility for industry personnel. Among those initiatives that DOD is exploring are (1) conducting a phased, periodic reinvestigation; (2) establishing a single adjudicative facility for industry; (3) reevaluating investigative standards and adjudicative guidelines; and (4) implementing an automated verification process for identifying and validating industrial security clearance requirements. These initiatives could, however, face implementation obstacles, such as the need to change governmentwide regulations.

Contents

Letter		1
	Results in Brief	3
	Background	5
	DOD's Backlog for Industry Personnel Was Roughly 188,000 Cases, and the Time Needed for the Clearance Process Has Increased	10
	Impediments Hinder Elimination of the Backlog and Reduction of Time Needed to Conduct an Investigation and Determine Eligibility for a Clearance	18
	DOD Is Considering Several Initiatives to Decrease the Backlog and Time Needed to Obtain a Security Clearance	31
	Conclusions	36
	Recommendations for Executive Action	38
	Agency Comments and Our Evaluation	38
Appendix I	Scope and Methodology	41
Appendix II	Excerpts from the Adjudicative Guidelines for Determining Eligibility for Access to Classified Information	44
Appendix III	Comments from the Department of Defense	46
Related GAO Products		53
Tables		
	Table 1: Information Gathered in Conducting an Investigation to Determine Eligibility for a Security Clearance	9
	Table 2: Comparison of Backlog Sizes As of September 30, 2003, and March 31, 2004	13
	Table 3: Average Number of Days Needed to Conduct an Investigation and Determine Eligibility for a Security Clearance for Industry Personnel, Fiscal Years 2001-2003	15

Table 4: Increase in the Average Number of Days Needed to Conduct an Investigation and Determine Eligibility for a Security Clearance for Industry Personnel, Fiscal Years 2001-2003	16
Table 5: Number of Clearance-Eligibility Determinations for Industry Personnel, Fiscal Years 2001-2003	20
Table 6: Increase in the Number of Clearance-Eligibility Determinations for Industry Personnel, Fiscal Years 2001-2003	20
Table 7: Proposed Phase 1 and Phase 2 Sources of Information for a Phased Reinvestigation	32

Figures

Figure 1: DOD's Personnel Security Clearance Process for Industry Personnel	7
Figure 2: Estimated Sizes of Industry Personnel and DOD-wide Backlogs and Time Frames Used to Determine Backlogs, as of September 30, 2003	12

Abbreviations

ACES	Automated Continuing Evaluation System
CAF	central adjudication facility
DD	Department of Defense (form)
DISCO	Defense Industrial Security Clearance Office
DOD	Department of Defense
DOHA	Defense Office of Hearings and Appeals
DSS	Defense Security Service
FBI	Federal Bureau of Investigation
JPAS	Joint Personnel Adjudication System
NACLC	national agency check/local agency check/credit check
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operating Manual
NSC	National Security Council
OPM	Office of Personnel Management
OUSD (I)	Office of the Under Secretary of Defense for Intelligence
PERSEREC	Defense Personnel Security Research Center
PR	periodic reinvestigation
PSI	personnel security investigation
PSWG	Personnel Security Working Group
SAP	special access program
SCI	sensitive compartmented information
SOR	statement of reasons
SSBI	single-scope background investigation
SSBI-PR	single-scope background investigation-periodic reinvestigation
TS PR	top secret periodic reinvestigation
TS/SCI	top secret/sensitive compartmented information

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



G A O

Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

May 26, 2004

The Honorable Tom Davis
Chairman
Committee on Government Reform
House of Representatives

The Honorable Christopher Shays
Chairman
Subcommittee on National Security,
Emerging Threats and International Relations
Committee on Government Reform
House of Representatives

As a result of an increased awareness of threats to our national security stemming from the terrorist attacks on the United States on September 11, 2001, and increased efforts over the past decade to privatize federal jobs, individuals working for private industry are playing an increasingly larger role in national security work conducted by the Department of Defense (DOD) and other federal agencies. Some industry personnel hold jobs requiring access to classified information that were formerly held by military members and federal employees. These jobs allow them to work on classified programs and activities. 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.

To protect national security, the federal government must provide high-quality and timely security clearances. As part of the 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 expressed concerns about the security clearance backlog—overdue security clearance reinvestigations¹ that have not been requested and new investigations and adjudications that have not been completed within established time

¹ Reinvestigations are conducted after a period of years to determine whether an individual's security clearance should be renewed.

frames—and the amount of time it takes DOD to conduct an investigation and determine eligibility for a security clearance for industry personnel.

As our previous work has shown, backlogs and delays in obtaining a security clearance historically have been problems for DOD, and they affect industry personnel as well as military members and federal employees.² 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.³ The impediments and recommendations apply to industry personnel as well as military members and federal employees. Likewise, the House Committee on Government Reform recently documented problems with DOD's personnel security clearance program and recommended changes to, among other things, reduce the backlog.⁴

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 the Office of Personnel Management (OPM).⁵ However, as of May 6, 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.

² See U.S. General Accounting Office, *DOD Personnel Clearances: Preliminary Observations Related to Backlogs and Delays in Determining Security Clearance Eligibility for Industry Personnel*, [GAO-04-202T](#) (Washington, D.C.: May 6, 2004); *DOD Personnel: More Consistency Needed in Determining Eligibility for Top Secret Clearances*, [GAO-01-465](#) (Washington, D.C.: Apr. 18, 2001); *DOD Personnel: More Actions Needed to Address Backlog of Security Clearance Reinvestigations*, [GAO/NSIAD-00-215](#) (Washington, D.C.: Aug. 24, 2000); and *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 Clearances: DOD Needs to Overcome Impediments to Eliminating Backlog and Determining Its Size*, [GAO-04-344](#) (Washington, D.C.: Feb. 9, 2004).

⁴ 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).

⁵ Pub. L. No. 108-136, § 906, (Nov. 24, 2003).

In response to your request, we reviewed the process that DOD uses to determine security clearance eligibility for industry personnel. As agreed with your offices, our objectives in this report concerning industry personnel clearances are to (1) describe the size of the security clearance backlog and changes during the last 3 fiscal years in the amount of time it takes to conduct an investigation and determine eligibility for a clearance, (2) identify reasons for the backlog and for delays in conducting investigations and determining eligibility, and (3) evaluate initiatives that DOD could take to eliminate the backlog and decrease the delays.

In conducting this review, we examined DOD's 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 analyzed data from the Case Control Management System's database, which manages the collection and dissemination of personnel security data from receipt of personnel security history to the monitoring, closing, transmitting, and maintaining of personnel security records. We assessed the reliability of the Case Control Management System's data used to determine the extent of the backlog and the time needed to conduct an investigation and determine eligibility for a clearance and determined that the data for fiscal years 2001 and thereafter were sufficiently reliable for the purpose of this report. In addition, we reviewed the methodology, sampling, and modeling techniques used in the Defense Personnel Security Research Center's reports on various DOD initiatives relating to the clearance process. We conducted our review from July 2003 through May 2004 in accordance with generally accepted government auditing standards. Additional information on our scope and methodology can be found in appendix I.

Results in Brief

As of March 31, 2004, DOD's security clearance backlog for industry personnel was roughly 188,000 cases, and the time needed to conduct an investigation and determine eligibility for a clearance had increased by 56 days during the last 3 fiscal years. 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 conduct an investigation and determine clearance eligibility for industry personnel increased from 319 days to 375 days. Delays in conducting an investigation and obtaining eligibility for a clearance can increase national security risks, 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 conduct an investigation and determine eligibility for a security clearance for industry personnel. Impediments that affect the security clearance program for industry overlap those that affect the DOD-wide program. As we reported in our February 2004 report, these impediments include large investigative and adjudicative workloads that are inaccurately projected.⁶ These large workloads stem from the large number of clearance requests in recent years and an increase in the proportion of requests requiring top secret clearances, which take longer and are more expensive to complete than secret clearances. The inaccurate forecasts for both the number and type of security clearances needed for industry personnel make it difficult for DOD to plan ahead and to size its investigative and adjudicative workforce to handle the workload. 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. In addition, the effects of past conditions—the backlogs themselves, problems with DOD's automated system for managing investigations, and additional national investigative requirements—are still being felt. Furthermore, DOD does not have a management plan to address the impediments in a comprehensive and integrated manner.

DOD and industry association officials have suggested a number of initiatives to reduce the backlog and the amount of time needed to conduct an investigation and determine eligibility for a security clearance. Among the steps that DOD is exploring are conducting a phased periodic reinvestigation, establishing a single adjudicative facility for industry, reevaluating investigative standards and adjudicative guidelines, and implementing an automated verification process for identifying and validating industrial security clearance requirements. Even if these initiatives prove promising, they face obstacles that could prevent or limit

⁶ See [GAO-04-344](#).

their implementation. For example, implementation of the phased periodic reinvestigation would require using a process that does not comply with existing governmentwide regulations.

We are making the following four recommendations to improve DOD's ability to eliminate security clearance backlogs for industry personnel and reduce the amount of time required to conduct an investigation and determine eligibility for a clearance: (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 addition, we made recommendations in our February 2004 report on security clearances DOD-wide that are important for industry personnel.⁷ Matching workforce sizes to workloads and completing the implementation of the DOD-wide automated system for adjudication management were among those recommendations.

In commenting on a draft of this report, DOD fully concurred with three of our four recommendations and partially concurred with our recommendation to develop and implement an integrated, comprehensive management plan to eliminate the backlog and reduce delays. Also, in commenting on our recommendations, DOD noted that we gave little or no acknowledgement to the many significant initiatives under way and policy changes implemented by DOD in past years to expedite the security clearance process. Our evaluation of DOD's comments documented that we recognized the positive steps that DOD has taken along with the failures that contributed to a long-standing problem. DOD's comments and our evaluation of them are on page 39.

Background

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.⁸ Within OUSD (I), the Defense Security Service (DSS) is responsible for conducting background investigations and administering the personnel security investigations

⁷ See [GAO-04-344](#).

⁸ 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).

program for DOD and 22 other federal agencies that allows industry personnel access to classified information.⁹ Two offices are responsible for adjudicating cases involving industry personnel. DSS's Defense Industrial Security Clearance Office (DISCO) adjudicates cases that contain only favorable information or minor issues regarding security concerns (e.g., some overseas travel by the individual), and the Defense Office of Hearings and Appeals (DOHA) within the Defense Legal Services Agency adjudicates cases that contain major security issues (e.g., an individual's unexplained affluence or criminal history).¹⁰

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. The level of classification denotes the degree of protection required for information and the amount of damage that unauthorized disclosure could reasonably be expected to cause to national defense or foreign relations. For top secret information, the expected damage that unauthorized disclosure could reasonably be expected to cause is "exceptionally grave damage;" for secret information, it is "serious damage;" and for confidential information, it is "damage."¹¹ Individuals who need access

⁹ 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. The agencies that have entered into agreements with DOD for security services under the National Industrial Security Program are the (1) National Aeronautics and Space Administration, (2) Department of Commerce, (3) General Services Administration, (4) Department of State, (5) Small Business Administration, (6) National Science Foundation, (7) Department of the Treasury, (8) Department of Transportation, (9) Department of the Interior, (10) Department of Agriculture, (11) Department of Labor, (12) Environmental Protection Agency, (13) Department of Justice, (14) Federal Reserve System, (15) U.S. General Accounting Office, (16) U.S. Trade Representative, (17) U.S. International Trade Commission, (18) U.S. Agency for International Development, (19) Nuclear Regulatory Commission, (20) Department of Health and Human Services, (21) Department of Homeland Security, and (22) Department of Education. The Department of Energy and the Central Intelligence Agency are signatories of the National Industrial Security Program Operating Manual and thus have reciprocity with DOD under provisions of the manual. 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.

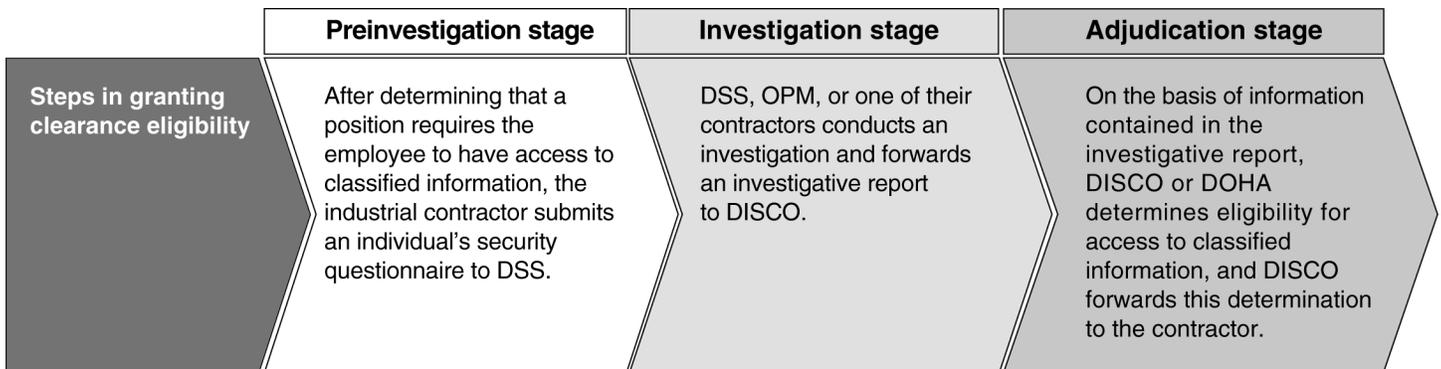
¹⁰ See Ralph M. Carney et al., *Quality Assurance in Defense Adjudication: An Adjudicator Workshop for Defining and Assessing Quality* (Monterey, Calif.: Defense Personnel Security Research Center, March 2003).

¹¹ *Classification of National Security Information*, 5 C.F.R. §1312.4 (2003).

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.¹²

To ensure the trustworthiness, judgment, and reliability of industry personnel in positions with access to classified information, DOD relies on a three-stage personnel security clearance process. (See fig. 1.) This process, which is essentially the same for industry personnel as it is for military members and federal employees, entails (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 a reinvestigation; and (3) using the investigative report to determine eligibility for access to classified information—a procedure known as “adjudication.”

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



Sources: DSS and DOHA.

Note: Cases involving sensitive compartmented information (see footnote 38) access are sent through the requesting agency’s central adjudication facility for adjudication.

In the preinvestigation stage, if a position requires a clearance, then the industrial contractor must request an investigation of the individual. The request could be the result of needing to fill a new position for a recent contract, replacing an employee in an existing position, renewing the clearance of an individual who is due for reinvestigation, or processing a request for a future employee (up to 180 days) in advance of the hiring

¹² *Adjudicative Guidelines for Determining Eligibility for Access to Classified Information*, 32 C.F.R. Part 147, Subpart B, Attach. A and Attach. C (2003).

date. Once the requirement for a security clearance is established, 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 OPM.

In the investigation stage, DSS, OPM, or one of their contractors conducts the actual investigation of the industry employee by using standards that were established governmentwide in 1997¹³ and implemented by DOD in 1998.¹⁴ 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 being conducted. For either an initial investigation or a reinvestigation for a confidential or secret clearance, investigators gather much of the information electronically. For a top secret clearance, investigators gather additional information that requires much more time-consuming efforts, such as traveling, obtaining police and court records, and arranging and conducting interviews. DSS's Personnel Investigations Center forwards the completed investigative report to DISCO.

¹³ 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.

¹⁴ 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 in Conducting an Investigation to Determine Eligibility for a Security Clearance

Type of information gathered	Type of security clearance		
	Confidential or secret	Top secret	
	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 the Federal Bureau of Investigation, military records centers, Department of the 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: DSS.

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 determined to be an “issue” case—a case containing information that might disqualify an individual for a clearance (e.g., foreign connections or drug- or alcohol-related problems)—then DISCO forwards the case to DOHA adjudicators for the clearance-eligibility decision. Regardless of which office renders the adjudication, 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 (see app. II).¹⁵ DISCO and DOHA serve as central adjudication facilities for industry personnel, whereas DOD uses eight other central adjudication facilities to approve, deny, or revoke eligibility for a security clearance for military members and federal employees.

DOD’s Backlog for Industry Personnel Was Roughly 188,000 Cases, and the Time Needed for the Clearance Process Has Increased

DOD’s security clearance backlog for industry personnel was roughly 188,000 cases, and the time needed to conduct an investigation and determine eligibility for a clearance had increased by 56 days during the last 3 fiscal years. As of March 31, 2004, DSS identified more than 61,000 overdue but not submitted reinvestigations and about 127,000 investigations or adjudications that had been started but not completed within set time frames. From fiscal year 2001 through fiscal year 2003, the average time that it took to conduct an investigation and determine clearance eligibility for industry personnel increased from 319 days to 375 days. DOD’s delays in conducting an investigation and determining clearance eligibility can, among other things, increase national security risks and the costs to the federal government of contractor performance on defense contracts.

¹⁵ The White House, “Implementation of Executive Order 12968,” Memorandum (Washington, D.C.: Mar. 24, 1997). This memorandum approves the adjudicative guidelines, temporary eligibility standards, and investigative standards required by Executive Order No. 12968, *Access to Classified Information*, Aug. 2, 1995.

Industry Personnel Backlog Was Roughly 188,000 Cases

As of March 31, 2004, the industry personnel backlog 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. For the 25,000 completed investigations awaiting adjudication, DSS found that over 19,000 of the cases were at DISCO and more than 6,300 of the cases were at DOHA. However, as of March 31, 2004, DOHA independently reported that it had eliminated its adjudication backlog. A complicating factor in determining the size of the industrial personnel backlog is that the backlog may be underestimated, since DSS had opened relatively few cases between October 1, 2003, and March 31, 2004, in anticipation of the authorized transfer of the investigative function from DSS to OPM.¹⁶ DSS had received, but not opened, almost 69,200 new industry personnel requests received in the first half of fiscal year 2004. Cases received in fiscal year 2004, which have already exceeded the set time frames for completing the investigation, are included in the 101,000 backlogged investigations identified above.

To view the industry personnel backlog in its proper context, we compared this backlog to the DOD-wide clearance backlog as of September 30, 2003, the date of the most recent DOD-wide data. For the preinvestigation stage, DOD did not know the total number of personnel DOD-wide with overdue requests for reinvestigation that had not been submitted—even though their clearances exceeded the governmentwide time frames for submitting reinvestigations.¹⁷ (See fig. 2.) Any request for a reinvestigation that has not been submitted within a specified time frame is overdue and considered part of the backlog. As noted in our February 2004 report, DOD could not estimate the number of military members and federal employees who had not requested a reinvestigation.¹⁸ Similarly, in a prior report, we indicated that DOD estimated its backlog of overdue but not submitted reinvestigations at 300,000 cases in 1986 and 500,000 cases in 2000.¹⁹ Because DOD's Case Control Management System has limited query capability, DOD was unable to identify the number of overdue

¹⁶ DSS investigators began training on OPM's case management system and investigative procedures and working on fiscal year 2004 requests in February 2004 (the fifth month of fiscal year 2004).

¹⁷ See [GAO-04-344](#).

¹⁸ See [GAO-04-344](#).

¹⁹ See [GAO/NSIAD-00-215](#).

but not submitted industrial personnel reinvestigations as of September 30, 2003. Although this system can identify overdue reinvestigations for industry personnel when queried at a specific point in time, it does not allow DOD to identify the number of military members and federal employees whose reinvestigations are overdue but not submitted at any time.

Figure 2: Estimated Sizes of Industry Personnel and DOD-wide Backlogs and Time Frames Used to Determine Backlogs, as of September 30, 2003

	Preinvestigation stage	Investigation stage	Adjudication stage
Steps in granting clearance eligibility	After determining that a position requires the employee to have access to classified information, the industrial contractor submits an individual's security questionnaire to DSS.	DSS, OPM, or one of their contractors conducts an investigation and forwards an investigative report to DISCO.	On the basis of information contained in the investigative report, DISCO or DOHA determines eligibility for access to classified information, and DISCO forwards this determination to the contractor.
Estimated size of industry backlog on September 30, 2003	There were an unknown number of requests for reinvestigation not submitted within prescribed time limits.	There were roughly 44,600 submitted requests for either an initial investigation or a reinvestigation not completed within prescribed time limits.	There were roughly 17,300 cases, including 12,800 completed investigations awaiting adjudication at DISCO and almost 4,500 cases awaiting adjudication at DOHA.
Estimated size of DOD-wide backlog on September 30, 2003	There were an unknown number of requests for reinvestigation not submitted within prescribed time limits.	There were roughly 270,000 submitted requests for either an initial investigation or a reinvestigation not completed within prescribed time limits.	There were roughly 90,000 completed investigations not adjudicated within prescribed time limits.
Criteria used to identify industry cases as backlogged	Criteria are 5 years for top secret, 10 years for secret, and 15 years for confidential clearances.	DSS's criteria are 75 days for an initial secret investigation, 120 days for an initial top secret investigation, and 180 days for a secret or top secret reinvestigation.	For DISCO, criteria are 3 days for initial clearances and 30 days for reinvestigations. For DOHA, it is the number of cases on hand that exceeds a steady workload of adjudicating 2,150 cases per month within 30 days

Sources: DOD (data); GAO (analysis).

The size of the total DSS-estimated backlog for industry personnel doubled during the 6-month period ending on March 31, 2004. Table 2 compares the sizes of the investigative and adjudicative backlogs at the end of fiscal year 2003 with the end of the first-half of fiscal year 2004. 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

Type of backlog	Estimated number of backlogged cases for industry personnel		Increase in 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.

As of September 30, 2003, 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. (See fig. 2.) DSS's time frames for completing investigations range from 75 days to 180 days, depending on the investigative requirements.²⁰ For instance, an initial secret investigation is required to be completed within 75 days, while a secret or top secret reinvestigation has to be completed within 180 days. Some requests for investigations receive priority over other requests. For example, requests for initial clearances receive priority over requests for reinvestigations, since individuals awaiting initial clearances cannot work whereas individuals who already have clearances that are due for reinvestigation can continue to work.

²⁰ 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.

As of September 30, 2003, the estimated size of the adjudicative backlog for industry personnel totaled roughly 17,300 cases. This number represented 19 percent of the roughly 93,000 cases in the DOD-wide adjudicative backlog on that date. Of the 17,300 industry personnel cases, some 12,800 were awaiting adjudication at DISCO (most of which were reinvestigations) and the remaining 4,500 cases were awaiting adjudication at DOHA. As of March 31, 2004, DOHA independently reported that it had totally eliminated this backlog of cases that had been awaiting initial adjudication by its security specialists. Typically, about 14 to 20 percent of the cases received by DISCO are eventually sent to DOHA for adjudication. As shown in figure 2, DISCO and DOHA use different time frames for identifying cases as backlogged. For example, DISCO uses 3 days for initial clearances and 30 days for reinvestigations, while DOHA uses different time frames on the basis of the number of cases on hand for 30 days that exceed a steady workload of 2,150 cases each month. If DISCO's time frames were applied to investigations awaiting adjudication at DOHA, then DOHA's backlog would have been larger than that reported at the end of fiscal year 2003.

Average Time for Clearance Process Increased to More Than 1 Year for Industry Personnel

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 rose from 319 days to 375 days, an increase of 18 percent. (See tables 3 and 4.) In other words, during fiscal year 2003, industry personnel waited an average of more than 1 year from the time DSS received a personnel security questionnaire to the time that DISCO issued an eligibility determination.

Table 3: Average Number of Days Needed to Conduct an Investigation and Determine Eligibility for a Security Clearance for Industry Personnel, Fiscal Years 2001-2003

Fiscal year	Average number of days to conduct an investigation and determine eligibility for a security clearance for industry personnel ^a		
	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 the Case Control 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 Control Management System and ending when DISCO notified the industrial contractor of the DISCO or DOHA adjudicators' decisions to determine eligibility for a clearance.

^aIncludes investigative time and DISCO review time.

^bIncludes 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.

In fiscal year 2003, it took DOD an average of 332 days to determine eligibility for “clean” cases, that is, those that had little or no potential security issues. (See table 3.) By comparison, it took DOD an average of 615 days to complete “issue” cases that contained potentially more serious security matters.²¹ This time period included DSS’s investigation, DISCO’s identification of potential issues and its forwarding of an issue case to DOHA, DOHA’s need to request additional investigation in some instances, and DOHA’s adjudication of the case. The 615-day average for issue cases is an overestimate because of problems with DSS’s Case Control Management System. The system is unable to distinguish between the end of the investigative and adjudicative processes to determine eligibility for a clearance and the continuing appeals process that may follow the denial of a clearance request or the revocation of a clearance.

²¹ According to DOHA officials, the 615-day figure is misleadingly high, since it includes time spent awaiting further processing, cases sent back for further investigation, cases requiring more information from the individual, or the few cases requiring an appeal after denial or revocation of a clearance.

Table 4 shows that from fiscal year 2001 through fiscal year 2003, the average number of days it took to conduct an investigation and determine eligibility for a security clearance for industry personnel increased by 56 days, or 18 percent.

Table 4: Increase in the Average Number of Days Needed to Conduct an Investigation and Determine Eligibility for a Security Clearance for Industry Personnel, Fiscal Years 2001-2003

Increases from fiscal year 2001 through fiscal year 2003	Average number of days to conduct an investigation and determine eligibility for a security clearance for industry personnel ^a		
	All industry cases	Clean cases ^a	Issue cases ^b
Number of days	56	31	99
Percentage of days	18%	10%	19%

Sources: DISCO and the Case Control Management System.

^aIncludes investigative time and DISCO review time.

^bIncludes 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.

Delays Can Affect National Security and Contract Timeliness, Quality, and Cost

Delays in renewing security clearances for industry personnel and others who are doing classified work caused by the backlog can lead to a heightened risk of national security breaches. Such breaches involve the unauthorized disclosure of classified information, which can cause up to “exceptionally grave damage” to national security. 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.²²

In addition, delays in determining security clearance eligibility for industry personnel can affect the timeliness, quality, and cost of contractor performance on defense contracts. A 2003 Information Security Oversight

²² See Joint Security Commission II, *Report by the Joint Security Commission II* (Aug. 24, 1999), pp. 5-6. In 1999, the Deputy Secretary of Defense and the Director of Central Intelligence reconvened the Joint Security Commission to assess progress towards the goals recommended in the original February 1994 Joint Security Commission report and examine emerging security issues.

Office²³ report identified concerns about the length of time required to process industrial security clearances.²⁴ According to the report, industrial contractor officials who were interviewed said that delays in obtaining clearances cost industry millions of dollars per year and affect personnel resources.²⁵ Interviewees reported having difficulty in filling sensitive positions and retaining qualified personnel. The report also stated that delays in the clearance process hampered industrial contractors' ability to perform duties required by their contracts. According to industry contractors, these delays increased the amount of time needed to complete national-security-related contracts. In interviews we conducted during our review, 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. As a result, according to industry association officials, industrial contractors may not be performing government contracts with the most experienced and best-qualified personnel, thus diminishing the quality of the work. Moreover, 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 turn, the recruit's former company may need to backfill the position, as well as settle for a lower level of contract performance while a new employee is found, obtains a clearance,

²³ 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.

²⁴ See Information Security Oversight Office, *The National Industrial Security Program, Industry's Perspective: Making Progress, but Falling Short of Potential* (2003).

²⁵ The Information Security Oversight Office evaluated the effectiveness of the National Industrial Security Program by conducting a survey of 4,709 industrial contractors, of which 393 responded. To follow up on the findings, the office supplemented the survey with on-site interviews of industry facility security officers and other corporate security representatives at 52 industry facilities across the country to discuss their views and experiences. Because only 8 percent of the industrial contractors responded to the survey, we did not use the survey data. However, we did use information gathered during the on-site interviews as examples of some of the timeliness, quality, and cost issues facing industrial contractors, recognizing that the comments cannot be generalized to the experiences of all industrial contractors.

and is trained. 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. We were told that contractors might pass these operating costs on to the federal government—and the taxpayer—in the form of higher bids for defense contracts.

Impediments Hinder Elimination of the Backlog and Reduction of Time Needed to Conduct an Investigation and 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 conduct an investigation and determine eligibility for a clearance. Impediments—similar to those we identified DOD-wide in our February 2004 report—also affect industry personnel and 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 insufficient investigative and adjudicative workforces to handle the large workloads.²⁶ The underutilization of reciprocity is an impediment that industrial contractors cited as an obstacle to timely eligibility determinations. The effects of past conditions, such as the backlog itself, problems with DSS's Case Control Management System, and additional national investigative requirements, also have been identified by DOD officials as impediments 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.

Clearance Workloads Are Large and Inaccurately Projected DOD-wide

A major impediment is the large—but inaccurately projected—number of requests for security clearances for industry personnel, military members, and federal employees. A growing number of these requests are for top secret clearances, which require more effort to process. The large and inaccurately projected investigative and adjudicative workloads for industry personnel cases must be viewed in the context of increasing DOD-wide and governmentwide clearance requirements. The large number of requirements is found in the form of both the number of requests and a growing portion of the requests requiring top secret clearances. Also, DOD has been unable to accurately project the number

²⁶ See [GAO-04-344](#).

Large Number of Clearance Requests DOD-wide Taxes Overburdened Process

and type of clearances required for industry personnel. Additional inaccuracy—a potential surge in clearance requests—could result when the Joint Personnel Adjudication System (JPAS) is fully implemented and DOD is able to identify overdue but not submitted reinvestigations DOD-wide.²⁷

The large number of clearance requests that DOD receives annually taxes a process that already is experiencing backlogs and delays. These requests are for industry personnel, as well as for military members and federal employees. In fiscal year 2003, DOD submitted over 775,000 requests for investigations to DSS and OPM. This figure included almost 143,000 requests for investigations of industry personnel. According to OPM officials, OPM has received an unprecedented number of requests for investigations governmentwide since September 2001 and has identified this large number as the primary reason for delays in granting clearances.

Table 5 shows an increase in the number of DOD eligibility determinations for industry personnel made during each of the last 3 years.²⁸ 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. (See table 4.) In other words, the increase in the average wait time was small compared to the increase in the number of cases. Fiscal year 2001 is an important baseline for examining changes in clearance processing because (1) major problems with DSS's Case Control Management System had been largely corrected and (2) the end of fiscal year 2001 occurred shortly after the September 11, 2001, terrorist attacks, which prompted an increase in clearance requests.

²⁷ JPAS is DOD's automated system to maintain all security clearance (eligibility and access) and adjudication information for DOD contractor and government personnel.

²⁸ 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.

Table 5: Number of Clearance-Eligibility Determinations for Industry Personnel, Fiscal Years 2001-2003

Fiscal year	Number of clearance-eligibility determinations for industry personnel		
	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

Sources: DISCO and the Case Control Management System.

Table 6 shows that from fiscal year 2001 through fiscal year 2003, the number of clearance eligibility determinations for industry personnel increased by more than 63,000 cases, or 174 percent.

Table 6: Increase in the Number of Clearance-Eligibility Determinations for Industry Personnel, Fiscal Years 2001-2003

Increases from fiscal year 2001 through fiscal year 2003	Number of clearance-eligibility determinations for industry personnel		
	All industry cases	Clean cases	Issue cases
Number of cases	63,282	53,878	9,404
Percentage of cases	174%	162%	306%

Sources: DISCO and the Case Control Management System.

Proportion of Requests Requiring Top Secret Clearances Has Grown

Beginning with 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. As indicated earlier, top secret clearances require more information than that needed for secret clearances. According to OUSD (I), top secret clearances take 8 times more investigative effort to complete and 3 times more adjudicative effort to review than do secret clearances. In addition, a top secret clearance must be renewed twice as often—every 5 years instead of every 10 years for a secret clearance. The full effect of requesting a top secret, rather than a secret, clearance thus is 16 times the investigative effort and 6 times the adjudicative effort.

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

Inaccurate Projections for Clearance Workload Hamper Planning

13 times higher than the \$328 it would require to investigate an individual for a secret clearance.

DOD's inability to accurately estimate the number and type of clearance requests that it will have to process for industry personnel during the next fiscal year is part of a bigger DOD-wide workload-estimation problem. For fiscal year 2001, DOD estimated that it would receive about 850,000 requests for clearances DOD-wide; however, the actual number of submissions was 18 percent lower than estimated. In contrast, DOD estimated that it would receive about 720,000 and 690,000 new requests DOD-wide in fiscal years 2002 and 2003, respectively, but the actual numbers of submissions were 19 and 13 percent higher than expected.

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 and 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 background investigations and top secret reinvestigations, both of which require considerably more effort to process. Since fiscal year 2001, DSS has conducted an annual survey of security officers at cleared contractor facilities over which DSS has cognizance to obtain their best estimates of the number of background investigations they would require over the next 7 years.²⁹ Using those estimates and historical data, DSS then prepares its annual security clearance projections for industry personnel. For fiscal year 2003, DSS asked each facility for the number and types of clearances that they would need. DSS said that about 25 percent of the approximately 11,000 cleared contractor facilities voluntarily responded to this request, but that 80 to 90 percent of the facilities with the largest dollar contracts responded. DSS officials attributed the inaccurate projection estimate to the use of some industry employees on more than one contract and often

²⁹ Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001, Pub. L. No. 106-398 (Oct. 30, 2000). This legislation amends 10 U.S.C. §1564 by directing DOD to quantify their requirements for background investigations necessary for granting security clearances for DOD personnel and industry personnel engaged in sensitive duties that are critical to the national security.

for different defense agencies; the movement of employees from one company to another; and unanticipated world events, such as the September 11, 2001, terrorist attacks. Currently, DSS does not receive data from DOD's acquisition community that issues the contracts—primarily military service and defense agency acquisition managers—to help DSS more accurately forecast the number and type of industrial personnel security clearances that would be required to implement or support their particular acquisition programs and activities.

DOD is developing a plan to link the number of investigations required for contract performance to an electronic database with personnel clearance information, and to require that the contracting officer authorize the number and type of investigations required. According to DOD, this will allow DSS to better monitor requirements and tie them to the budget process. Also, linking the electronic personnel clearance information database with the contract database maintained by the acquisition community would tie the security clearance process more closely to the acquisition process.

Surge in Requests May Occur
When JPAS Is Fully
Implemented DOD-wide

DOD may experience a surge in security clearance requests DOD-wide when JPAS is fully implemented.³⁰ This system will enable DOD to identify overdue reinvestigations that have not been submitted. However, any surge in the number of unexpected reinvestigations may be identified too late to have the extra workload planned and budgeted for the next fiscal year.

DOD's inability to fully anticipate the number of reinvestigations that will be submitted is the result of continued delays in implementing JPAS, a system that DOD's Chief Information Officer has identified as a mission critical system. In response to a recommendation in our August 2000 report,³¹ DOD said that JPAS would be implemented in fiscal year 2001 and would provide an automated means of tracking and counting overdue but not submitted requests for reinvestigations. At the time of our February 2004 report, which again recommended the implementation of JPAS,

³⁰ DOD officials suggested that the number of overdue but not submitted reinvestigations could decrease for industry personnel, since JPAS would identify some personnel in the system more than once or others who no longer needed a security clearance. We continue to be concerned about a possible surge in requests because sufficient data are not available to determine accurately the number of unsubmitted requests for industry personnel as well as military members and federal employees.

³¹ See [GAO/NSIAD-00-215](#).

OUSD (I) officials said that they expected to fully implement JPAS during January 2004.³² Currently, OUSD (I) officials project that JPAS will be fully implemented sometime in fiscal year 2004.

Insufficient Investigative and Adjudicative Staff Cannot Handle Large Workloads

Insufficient investigative and adjudicative workforces, given the current and projected workloads, serve as 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.³³ DOD—like the rest of the federal government—is competing for a limited number of investigative staff. In contrast, DOD has more control over its adjudicative capacity and has taken steps to increase those resources.

Too Few Investigative Staff Are Available to Meet Government and DOD Needs

The limited number of investigative staff available to process requests from DOD and other government agencies hinders DOD's efforts to eliminate the backlog and issue timely clearances for industry personnel. 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.³⁴ However, 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, slightly more than half as many as needed.³⁵

In addition to having too few investigators, DOD may experience a short-term decrease in productivity in the near future as DSS investigative employees are pulled away from their investigations to receive training on OPM's case management system and investigative procedures. 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

³² See [GAO-04-344](#).

³³ See [GAO-04-344](#).

³⁴ OPM has estimated that DOD and OPM account for 80 percent of the investigations conducted for the federal government.

³⁵ See [GAO-04-344](#).

Too Few Adjudicative Staff
Are Available to Meet Industry
Needs

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 productivity 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.

Similarly, an adjudicative backlog of industry personnel cases developed because DISCO and DOHA did not have an adequate number of adjudicative personnel on hand. DOD personnel and industry officials identified several reasons why adjudicator staff have not been able to process requests within their established time frames. These include an increase in the number of investigations being sent to DISCO and DOHA as a result of the September 11, 2001, terrorist attacks and the larger number of completed investigations stemming from DOD's contract with OPM and private-sector investigation companies. The adjudicative backlog also resulted from problems in the operations of DSS's Case Control Management System.

DISCO and DOHA have taken steps to decrease the backlog and delays by augmenting their adjudicative staff. As of September 30, 2003, DISCO had 56 nonsupervisory adjudicators on board, and 6 additional nonsupervisory adjudicator applicants are currently undergoing investigations for their security clearances. By contrast, only 33 nonsupervisory adjudicators were available in 2001. To achieve part of this increase in the number of adjudicators, DISCO moved nonadjudicative customer service employees into adjudicative positions and filled the vacated positions with contract personnel. In addition, DISCO authorized overtime for its adjudicative staff. As of September 30, 2003, DOHA had 23 permanent federal adjudicators as well as 46 temporary adjudicators hired specifically to help reduce its adjudicative backlog. In 2001, after DOHA identified a growing adjudicative workload of industry personnel cases that exceeded its capacity, it received authority to hire 46 additional term-appointment adjudicators. After establishing this plan to eliminate its backlog of cases awaiting initial adjudication by its security specialists, DOHA requested authority to hire additional permanent adjudicators to ensure that a backlog would not recur.

Reciprocity of Access Is Not Fully Utilized

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 already overburdened investigative and adjudicative staff.³⁶ According to DOD and industry officials, a 2003 Information Security Oversight Office report on the National Industrial Security Program,³⁷ 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 programs³⁸ within DOD or transferring clearances and access from DOD to 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 for many of these programs simultaneously.³⁹

The extent of the problems that are caused by the lack of full reciprocity is unknown. In 2001, the Defense Personnel Security Research Center proposed collecting quantitative data on the number and type of personnel affected by reciprocity. However, the center determined that the differences in how the various agencies handled tracking these personnel situations proved so great and the databases they used so various that center researchers could not overcome these incompatibilities in the time

³⁶ 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.

³⁷ See Information Security Oversight Office, *The National Industrial Security Program, Industry's Perspective: Making Progress, but Falling Short of Potential* (2003).

³⁸ 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.

³⁹ See Defense Personnel Security Research Center, *Reciprocity: A Progress Report*, PERSEREC Technical Report 04-2 (Monterey, Calif.: Apr. 1, 2004).

and with the resources they had for the study. This situation has occurred despite the establishment in 1997 (and implementation by DOD in 1998) of governmentwide investigative standards and adjudicative guidelines. In 1999, the interagency Joint Security Commission II noted, “With these standards and guidelines in place, there is no longer a legitimate reason to investigate or readjudicate when a person moves from one agency’s security purview to another.”⁴⁰ More recently, the chair of the federal interagency Personnel Security Working Group indicated that the lack of full reciprocity is a major concern governmentwide, not just within DOD.

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 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) type of polygraph tests, and (3) refusal to accept adjudication decisions made by other agencies. Industry association officials stated that these access problems are becoming more common, especially for firms with multiple contracts with different intelligence agencies.

Industry officials identified reciprocity concerns for the following situations, among others:

- *Sensitive compartmented information and special access programs*—The DOD directive that establishes policy, responsibilities, and procedures for industry employee clearances explicitly provides that the directive “[d]oes not apply to cases for access to sensitive compartmented information or a special access program.”⁴¹ The procedures used in determining access to sensitive compartmented information and special access programs are different from those used in the normal clearance process. These procedures may involve applying more selective and stringent investigative and adjudicative criteria. The reciprocity of sensitive compartmented information eligibility determinations is left up

⁴⁰ See Joint Security Commission II, *Report by the Joint Security Commission II* (Aug. 24, 1999), p. 2.

⁴¹ DOD Directive 5220.6, *Defense Industrial Security Clearance Review Program*, § 2.6 (Apr. 20, 1999).

to each organization or agency that may have additional investigative requirements that must be met (e.g., a polygraph test) prior to granting access. While DOD requires that special access program eligibility determinations for military members and federal employees be mutually and reciprocally accepted by all DOD components, this requirement does not apply to industry personnel.

DOD components and some of the agencies serviced by DISCO do not always accept the interim clearances that DISCO issues to industry employees. DISCO provides interim clearances when an individual's case does not identify any potential security issues after a review of initially gathered information. DISCO reported that it issues interim clearances to about 95 percent of those industry personnel applying for a secret clearance within 3 days of receiving the clearance request. However, according to industrial contractors, their ability to use industry personnel with interim clearances on some contracts but not on others limits their staffing options. In addition, 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.⁴²

Industry associations told us that intelligence agencies do not accept DOD's waivers, even with a letter of consent from the employee's former company or a verification letter by the agency that requested the original investigation and granted the employee the clearance. To eliminate the need to perform another investigation, the Office of the Secretary of Defense may use a waiver to reinstate or convert a security clearance under certain circumstances.⁴³ For example, a security clearance can be converted if an individual leaves the federal government and subsequently begins to work for an industrial contractor, provided that (1) no more than 24 months have elapsed since the date the clearance was terminated,

⁴² 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.

⁴³ DOD Manual 5220.22-M, *National Industrial Security Program Operating Manual* (May 1, 2000), p. 2-2-4.

(2) there is no known adverse information, and (3) the most recent investigation meets both the scope and completion time frame for the clearance being reinstated. By using waivers for reinstatements and conversions, DOD can eliminate the need to perform another investigation.

- *Smith Amendment*—Many DOD and industry officials view the Smith Amendment⁴⁴ as an impediment to reciprocity because people who once worked for DOD or other agencies may not be eligible to work for DOD when it is time to renew their clearance because of selected potential security issues. The Smith Amendment, which applies only to DOD, specifies that DOD should not grant or renew a clearance for anyone who (1) has been sentenced to imprisonment for a term exceeding 1 year, (2) is an unlawful user of or is addicted to a controlled substance, (3) is mentally incompetent, or (4) has been discharged or dismissed from the military under dishonorable conditions. Therefore, a clearance previously granted by another federal agency or through DOD would be ineligible for a subsequent DOD clearance if one or more of the four prohibitions were applicable. However, the Secretary of Defense or one of the Service secretaries may authorize an exception to the Smith Amendment prohibitions, but only in cases where the individual seeking the clearance has been sentenced to imprisonment for a term exceeding 1 year or has been dishonorably discharged from the Armed Forces.

Ordinarily, the adjudicators are to consider mitigating factors and available, reliable information about the person—past and present, favorable and unfavorable—in reaching an “overall common sense” clearance-eligibility determination that gives careful consideration to the 13 adjudicative guidelines. (See app. II.) According to the guidelines, any doubt about whether a clearance for access to classified information is consistent with national security is to be resolved in favor of national security. However, under the Smith Amendment, such mitigating factors should not be considered when one or more of the four elements are present in the investigative report on a person applying for a clearance through DOD—unless the Secretary of Defense or one of the Service secretaries issues a waiver.

⁴⁴ 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).

Effects of Past Conditions Still Being Felt

A number of past conditions also serve as impediments to issuing timely eligibility determinations for industry personnel. The backlogs themselves contribute to delays because most new requests for investigations remain largely dormant until earlier requests are completed. Backlogged cases might delay the start of an initial secret clearance, for instance, until 60 days after it is received by DSS. In such a hypothetical situation, DSS would have only 15 days, rather than the full 75 days, to complete the investigation before having the case labeled as “backlog.” Similarly, the adjudicative backlog might lead to a delay in reviewing new investigative reports, thereby increasing the likelihood that a new adjudication will be categorized as “backlog” before an eligibility determination is provided.

In addition, problems with DSS’s Case Control Management System during fiscal years 1999 and 2000 affected the processing of security clearances in subsequent years. These problems included limiting the dissemination of leads to investigative staff and, thereby, limiting the flow of completed cases to adjudication facilities, such as DISCO and DOHA. Although DSS officials indicate that the Case Control Management System problems have been corrected, the February 2004 interagency agreement between DSS and OPM allows DOD to replace that system with OPM’s case management system. An OUSD (I) official said that DOD estimates it will save about \$100 million over 5 years by avoiding the need to update and maintain DSS’s Case Control Management System.

According to DSS officials, additional national investigative requirements, which were implemented by DOD in 1998, have strained nationwide investigative resources.⁴⁵ For instance, the current requirement for a secret clearance calls for investigative staff to conduct national agency checks, local area checks, and a credit check. Previously, a secret clearance required only national agency checks. DOD has had over 5 years to address this issue and allocate sufficient resources to handle the additional requirements.

⁴⁵ See The White House, “Implementation of Executive Order 12968,” Memorandum (Washington, D.C.: Mar. 24, 1997).

Lack of Overall Management Plan Exacerbates Clearance Backlog and Delays

Currently, 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. DOD has a plan to engineer a business process for personnel security, transform DSS as an agency, complete and closeout DSS's old investigative work, and decommission DSS's Case Control Management System.⁴⁶ DOD also has a transition plan to transfer DSS's investigative function to OPM. The terms and conditions of that transfer are contained in the *Memorandum of Understanding* between DOD and OPM (Jan. 24, 2003). Because the transition has not occurred yet, DSS signed the *Interagency Agreement* with OPM (Feb. 6, 2004) 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. Finally, DSS has a draft *Fiscal Year 2004 Performance Plan* (Mar. 25, 2004) that is intended to serve as an interim plan pending final implementation of DSS's strategic plan as a transformed agency. Rather than including specific performance measures seen in previous plans, this plan provides an accounting of milestones that must be achieved for the agency's transformation. None of these plans address eliminating permanently the investigative and adjudicative backlogs, reducing the delays in conducting investigations and determining eligibility for clearances, or overcoming the impediments. In addition, none of these plans address budgets, personnel resources, costs, or potential obstacles and options for overcoming the obstacles to eliminate the backlog and reduce the delays.

DOD's numerous plans do not include establishing processwide objectives and outcome-related goals; setting priorities; identifying resources; establishing performance measures; and providing milestones for reducing, and eventually eliminating, the backlog and delays. The principles of the Government Performance and Results Act of 1993 provide federal agencies with a basis for such a results-oriented framework that includes setting goals, measuring performance, and reporting on the degree to which goals are met.⁴⁷

⁴⁶ See OUSD (I), *Reengineering Personnel Security* (July 2003).

⁴⁷ Pub. L. No. 103-62 (Aug. 3, 1993).

DOD Is Considering Several Initiatives to Decrease the Backlog and Time Needed to Obtain a Security Clearance

DOD and industry association officials have suggested a number of initiatives to reduce the backlog and delays in conducting an investigation and 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.

- *Phased periodic reinvestigations could make staff available for more productive uses.* A phased approach to periodic reinvestigations involves conducting a reinvestigation in two phases; a more extensive reinvestigation would be conducted only if potential security issues were identified in the initial phase. Table 7 identifies proposed sources of information for both parts of a phased periodic reinvestigation. The more productive sources for investigative leads are shown in phase 1. Investigative staff would gather information from phase 2 sources only in those cases where potential security issues were uncovered in phase 1.

Table 7: Proposed Phase 1 and Phase 2 Sources of Information for a Phased Reinvestigation

Phase 1 sources	Phase 2 sources
Personnel Security Questionnaire	Listed reference interviews
Credit report	Developed reference interviews
Polygraph (if used)	Residence interviews
National agency check of subject	Residence records
National agency check of spouse/cohabitant	
Local agency checks	
Financial Center Title 31	
Reports received between reinvestigations	
Subject interview	
Employment interviews	
Ex-spouse interview	
Security records	
Security manager interview	
Medical records	
Medical interview	
Employment records	
Military records	
Public records	
All other sources not in Phase 2	

Source: Defense Personnel Security Research Center.

Recent research has shown that periodic reinvestigations for top secret clearances conducted in two phases can save at least 20 percent of the normal investigative effort with almost no loss in identifying critical issues for adjudication.⁴⁸ This research included phasing analyses conducted by the Defense Personnel Security Research Center with 4,721 reinvestigations for top secret clearances, a pilot test conducted by DSS, independent research at the Central Intelligence Agency and National Reconnaissance Office, and an evaluation of DSS's implementation of a phased reinvestigation in fiscal year 2003 conducted by the Defense

⁴⁸ 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).

Personnel Security Research Center. This research has shown that the most productive sources (phase 1 sources) can be used to identify investigations in which the least productive sources (phase 2 sources) are likely to yield issue information. Analyses showed a phased approach missed very little potential security issue information and identified all of the cases in which agencies took some form of action against individuals (e.g., a suspension of their clearance or warnings, monitoring, or reprimands). 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. Research conducted by the Defense Personnel Security Research Center suggests the phased periodic reinvestigation represents a way of balancing the risks of a rare missed issue and the costs associated with a normal reinvestigation. 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 could prevent the implementation or limit the use of this initiative. First, the phased reinvestigation does not comply with the *Investigative Standards for Background Investigations for Access to Classified Information (Standard C)*.⁴⁹ Currently, *Standard C* mandates the same investigative scope for all reinvestigations for top secret clearances, whereas the phased approach uses different standards for clean versus potential issue cases. Second, any change in *Standard C* would necessitate a corresponding change in the Code of Federal Regulations. Third, without modification of *Standard C*, reciprocity problems could result if some agencies use the phased reinvestigation and other agencies refuse to accept eligibility determinations based on it. DOD is now actively working to change *Standard C* so that a phased reinvestigation would be an option under the national standards.

⁴⁹ Approved by the National Security Council in 1997 as part of the *Common Investigative Standards*, the *Investigative Standards for Background Investigations for Access to Classified Information (Standard C)* establish when a reinvestigation must be conducted, specific investigative requirements, and when a reinvestigation may be expanded.

-
- *Single adjudicative facility for industry could reduce adjudicative time.* Under this initiative, DOD would consolidate DOHA's adjudicative function with that of DISCO to create a single adjudicative facility for all industrial contractor 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.

DOD's Senior Executive Council is considering this consolidation as part of a larger review of DOD's security clearance process. From 1991 through 1998, studies by the Defense Personnel Security Research Center, Joint Security Commission, and DOD Office of the Inspector General concluded that the present decentralized structure of DOD's adjudication facilities had drawbacks. Two of the studies recommended that DOD consolidate its adjudication facilities (with the exception of the National Security Agency).

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 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 could reveal efficiencies.* 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 to 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 1 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 Intelligence Authorization Act for Fiscal Year 2004 required the Secretary of Defense, Director of Central Intelligence, the Attorney General, and Director of OPM to jointly submit to Congress by February 15, 2004, a report on the utility and effectiveness of the current security background investigations and security clearance procedures of the federal government, including a comparison of the costs and benefits of conducting background investigations for secret clearances with the costs and benefits of conducting full field background investigations.⁵⁰ At the time of our report, the report mandated in the intelligence act had not been delivered to Congress.

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 *Common Investigative Standards*. In addition, the evaluation would need to be coordinated within DOD, intelligence agencies, and others.

- *Requirements-identification improvements could optimize resources and reduce backlog and delays.* This initiative would use an automated verification process to identify and validate security clearance requirements for industry personnel. DSS officials stated that a process to verify requirements could help DSS allocate investigative and adjudicative resources to projected workloads, thereby reducing the backlog and delays. DOD is considering implementing this initiative to help project the number and type of clearances that industry may need for a specific acquisition program. According to DSS officials, more stability is needed in workload projections to allow the government and industrial contractors to size their investigative workforces with the workload. This projection becomes more critical because the investigative function is labor-intensive and it can take 1 year to hire and train investigators before they are able to work independently. Implementing this initiative might require additional data gathering and reporting by DOD's acquisition community that issues contracts—primarily military service and defense agency acquisition managers, especially when contracts are being awarded. Although industry currently provides this information voluntarily, the acquisition community is not required to provide this information.

⁵⁰ Pub. L. No. 108-177, § 352 (Dec. 13, 2003).

-
- *Automated Continuing Evaluation System may result in additional workloads.* The last initiative involves testing and eventually implementing the Automated Continuing Evaluation System, which is being developed by the Defense Personnel Security Research Center. This automated assessment tool is designed to provide automated database checks and identify issues of security concern on cleared individuals between the specified periodic reinvestigations. The system does not require an individual to complete any additional paperwork before a query is undertaken. In addition, the system automatically notifies adjudication facilities when an individual with a security clearance engages in an act of security concern. This notification occurs sooner than is currently possible. The system underwent a large-scale pilot program in 2002 and was subsequently modified. Operational field testing began in April 2004. DOD officials acknowledge that the Automated Continuing Evaluation System alone would not help to eliminate the backlog and, in fact, may initially result in larger investigative and adjudicative workloads. However, they maintain that, when combined with the phased periodic reinvestigation, the system could help reduce workloads and the backlog, and ultimately improve personnel security.

This initiative would face some of the same obstacles as those raised for a phased periodic reinvestigation—the need to change governmentwide investigative standards and concerns about reciprocity.

Conclusions

The backlog of clearances for industry personnel and delays in conducting investigations and determining eligibility for a clearance must be considered in the larger context of DOD-wide backlogs and delays. Many of the impediments and initiatives identified in this report apply to both industry-specific and DOD-wide situations. Taken together, these impediments hamper DOD's ability to eliminate the security clearance backlog and reduce the amount of time it takes to determine clearance eligibility for industry personnel.

DSS is unable to accurately project the number and type of security clearances needed for industry personnel as well as military members and civilian employees. This makes it difficult to determine budgets and staffing for investigative and adjudicative workforces. Without close coordination and cooperation among all interested parties—OUSD (I), DOD components issuing the contracts, industrial contractors, and the acquisition community—inaccurate projections of the number and type of clearance requirements for industrial personnel could continue.

The reciprocity of security clearances within DOD has not been a problem for industry personnel; however, reciprocity for access to certain types of information and programs within the federal government has not been fully utilized. As a result, some who already have clearances issued by one agency face delays in starting to work on contracts for other agencies. In addition, the failure to utilize reciprocity unnecessarily increases the investigative and adjudicative workloads on the already overburdened investigative and adjudicative staff.

In recent years, DOD has reacted to the impediments in a piecemeal fashion rather than by establishing an integrated approach that incorporates objectives and outcome-related goals, sets priorities, identifies resources, establishes performance measures, and provides milestones for permanently eliminating the backlog and reducing delays. Without such an integrated, comprehensive plan, DOD's efforts to improve its process for conducting security clearance background investigations and adjudications for industry personnel will likely continue to proceed in a piecemeal fashion.

DOD and industry officials have suggested a number of initiatives that could help eliminate the backlog and reduce clearance delays. However, it remains unclear whether any single initiative—or combination of initiatives—can have a direct and immediate impact on the backlog or delays. 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 or limit the implementation of the initiatives.

We made recommendations in our February 2004 report on security clearances for DOD personnel that also apply to industry personnel.⁵¹ Among other things, we recommended that the Secretary of Defense direct the Under Secretary of Defense for Intelligence to (1) identify and implement steps to match the sizes of the investigative and adjudicative workforces to the clearance request workload and (2) complete the implementation of the Joint Personnel Adjudication System. In its written response on a draft of that report, DOD partially concurred with the first recommendation and concurred with the second recommendation. Since we have already recommended these actions in the larger context of DOD personnel, we are not repeating them in this report for industry personnel.

⁵¹ See [GAO-04-344](#).

Recommendations for Executive Action

To improve the security clearance process for industry personnel as well as for military members and federal employees, we recommend that the Secretary of Defense direct the Under Secretary of Defense for Intelligence to take the following four actions:

- improve the projections of clearance requirements for industrial personnel—both the number and type of clearances—by working with DOD components, industrial contractors, and the acquisition community to identify obstacles and implement steps to overcome them;
- work with DOD components and other agencies to eliminate unnecessary reciprocity limitations for industry personnel whose eligibility for a clearance is granted by DOD;
- develop and implement an integrated, comprehensive management plan to eliminate the backlog, reduce the delays in conducting investigations and determining eligibility for security clearances, and overcome the impediments that could allow such problems to recur; and
- analyze the feasibility of implementing initiatives designed to reduce the backlog and delays, prioritize the initiatives, and make resources available for testing and implementing the initiatives, which could include, but are not limited to, those evaluated in this report.

Agency Comments and Our Evaluation

In written comments on a draft of this report, DOD fully concurred with three of our four recommendations: improve projections of clearance requirements for industrial personnel, eliminate unnecessary reciprocity limitations, and analyze the feasibility of initiatives to reduce the backlog and delays. DOD partially concurred with our recommendation to develop and implement an integrated, comprehensive management plan.

In its partial concurrence, DOD noted that it had numerous plans to improve its process and said we did not identify why a single, comprehensive plan would improve its ability to achieve success. As our report points out, there are several reasons for the recommendation. Specifically, the plans that DOD provided to us often were missing details on budgets, personnel resources, costs, milestones with specific dates for accomplishment, identification of potential obstacles, and options for overcoming the obstacles if they should occur. Also, the use of multiple smaller plans does not provide DOD with a bigger picture of how it should strategically plan and prioritize its personnel and budget resources and actions required simultaneously in two or more plans. Continued use of piecemeal planning could result in a failure to recognize problems not yet addressed or planned actions that conflict with those being implemented—or planned as part of another effort. Moreover, DOD cited its plan to transfer DSS's investigative functions and personnel to OPM.

While the plan would result in DOD eliminating its *responsibility* for conducting the investigations, no new investigative personnel would result, if or when the transfer occurs. Therefore, it is not apparent how the transfer will help DOD eliminate its backlog and reduce clearance delays. DOD's failure to identify contingency actions if the transfer did not occur according to its plans already has delayed the start of nearly 70,000 investigations for industry personnel in fiscal year 2004. We continue to believe our recommendation has merit and should be implemented.

Also, in commenting on our recommendations, DOD made several points that need to be addressed. DOD noted that we gave little acknowledgement to the many significant initiatives under way and no acknowledgement to policy changes implemented by DOD in past years to expedite the process. Our report highlights several steps DOD has taken. First, we acknowledged actions that DOD has taken in recent years to address the backlog—and handle the 174 percent increase from fiscal year 2001 through fiscal year 2003 in the number of clearance eligibility determinations for industry personnel, such as contracting for additional investigative services, hiring more adjudicators, and authorizing overtime for adjudicative staff. Second, we discuss in some detail five significant initiatives that DOD is considering to reduce the backlog and delays. DOD noted that its initiatives “are gradually improving the process.” This DOD statement supports our conclusion that it remains unclear whether any of the initiatives—individually or collectively—can have a direct and immediate impact on the backlog or delays. Third, we acknowledged policy changes, but many of the changes were implemented from 4 to 18 years earlier—using waivers for clearance reinstatements and conversions to eliminate the need to perform another investigation (2000), implementing national investigative standards and adjudicative guidelines (1999), utilizing full reciprocity (1997), and granting of interim clearances to put industry personnel to work (1986). These positive steps must, however, be considered in the context of major concerns that remain. These concerns include the sizeable and long-standing backlog; the length of time needed to conduct an investigation and determine eligibility for a clearance, which now takes, on average, over 1 year to complete; the failure to implement JPAS throughout DOD with all of its intended design features, even though DOD said it would be implemented in fiscal year 2001; and DOD's declaration that its personnel security investigations program has been a systemic weakness since fiscal year 2000. We believe that our report presents a balanced representation of the improvements and the failures that contributed to a long-standing problem that can increase national security risks; affect the timeliness, quality, and costs of contractor performance on national-security-related contracts; and ultimately increase costs to the federal government.

DOD's comments are reprinted in appendix III. DOD also provided technical comments that we incorporated in the final report as appropriate.

We are sending copies of this report to other interested congressional committees. We also are sending copies to the Secretary of Defense; the Director, Office of Personnel Management; and the Director, Office of Management and Budget. We will make copies available to other interested parties upon request. This report also will be available at no charge on GAO's Web site at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-5559 or by e-mail at stewartd@gao.gov or contact Jack E. Edwards at (202) 512-8246 or by e-mail at edwardsj@gao.gov.

Mark A. Pross, James F. Reid, William J. Rigazio, and Nancy L. Benco made key contributions to this report.

A handwritten signature in black ink that reads "Derek B. Stewart". The signature is written in a cursive style with a large initial 'D'.

Derek B. Stewart, Director
Defense Capabilities and Management

Appendix I: Scope and Methodology

In conducting our review of the security clearance process for industry personnel, we visited key offices within the Department of Defense (DOD) that have responsibility for oversight and program management and implementation. We also met with selected industrial contractors and industry associations whose employees and members are affected by the DOD backlog and delays in conducting investigations and determining eligibility for security clearances. We conducted our work in Washington, D.C., at DOD, including the Office of the Under Secretary of Defense for Intelligence (OUSD [I]); Defense Security Service (DSS); and the Defense Office of Hearings and Appeals (DOHA); at the Office of Personnel Management; the Information Security Oversight Office at the National Archives and Records Administration; and at the Personnel Security Working Group of the National Security Council's Policy Coordinating Committee on Records Access and Information Security. We also conducted review work in Columbus, Ohio, at the Defense Industrial Security Clearance Office (DISCO) and DOHA; at Fort Meade, Maryland, at DSS's Personnel Investigations Center; and in Monterey, California, at the Defense Personnel Security Research Center.

We met with representatives of several industrial contractors, including Northrop-Grumman Corporation, Linthicum, Maryland, and Data Systems Analysts, Inc., and General Dynamics Advanced Information Systems in Arlington, Virginia. In addition, we held discussions with officials representing industry associations, including the Northern Virginia Technology Council and the National Classification Management Society in Washington, D.C.; via telephone with the Shipbuilders Council of America; with officials from the Information Technology Association of America, Arlington, Virginia; and with representatives from the Aerospace Industries Association and National Defense Industrial Association, Linthicum, Maryland.

To determine the size of the security clearance backlog and changes during the last 3 fiscal years in the amount of time it takes to conduct an investigation and issue a clearance eligibility determination, we met with DSS and DOHA officials to obtain the relevant data from the Case Control Management System and discussed their methods for determining what constitutes a backlog. As part of the process for estimating the backlog, we observed the steps used to process investigative and adjudicative information during our visits to the DSS Personnel Investigations Center, DISCO, and DOHA. During these site visits, we obtained information on the number of days required to complete an investigation or adjudication, the time frames for designating what constitutes an investigative or adjudicative backlog, and data reliability through questionnaires and

interviews. Our Applied Research and Methods team assisted us in reviewing the reliability of the databases used to determine the backlog. We also examined data for fiscal years 2001 to 2003 to track changes in how long it took industry personnel to obtain a clearance during those years. We discuss developments during the first half of fiscal year 2004, where appropriate, so that information is current as of March 31, 2004.

To identify the reasons or impediments for the backlog and delays in conducting investigations and issuing eligibility determinations, we reviewed reports by GAO, DOD Office of the Inspector General, House Committee on Government Reform, Defense Personnel Security Research Center, Information Security Oversight Office, and the Joint Security Commission II. We interviewed officials from DSS, DISCO, and DOHA and observed and reviewed their procedures. We also discussed impediments with officials of OUSD (I), the Defense Personnel Security Research Center, the Information Security Oversight Office, and the Chair of the Personnel Security Working Group of the National Security Council, as well as industry representatives. In addition, we reviewed these agencies' prior reports. Our Office of the General Counsel reviewed various public laws; executive orders; federal regulations; and DOD policy memorandums, directives, regulations, and manuals.

To identify additional steps that DOD could take to reduce the time needed to conduct investigations and issue eligibility determinations, we reviewed prior reports to identify previously suggested initiatives. We supplemented this information with discussions on the status of those previously identified steps, as well as ongoing initiatives, with both industry representatives and government officials. Where appropriate, our Applied Research and Methods team reviewed Defense Personnel Security Research Center reports to help ensure that the center's (1) approaches were methodologically sound, (2) sampling and statistical modeling techniques were sufficient, and (3) proposed empirically based procedural changes to DOD's security clearance process also were methodologically sound. The team also reviewed industry association survey results and evaluated the validity and reliability of the survey methodology and results.

We assessed the reliability of the data that were provided by DSS's Case Control Management System and used to determine the investigative and adjudicative backlog and the time needed to conduct an investigation and determine eligibility for a security clearance by (1) reviewing existing information about the data and system that produced them,

(2) interviewing agency officials knowledgeable about the data, and
(3) reviewing DISCO's and DOHA's responses to a detailed questionnaire about their information technology data reliability. We determined that the data for fiscal years 2001 and thereafter were sufficiently reliable for the purpose of this report.

The Case Control Management System also faced certain limitations, which had an impact on our findings. Although the Case Control Management System, which is used to obtain the backlog estimates, 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 Control Management System and ending when DISCO notified the industrial contractor of the DISCO or DOHA adjudicators' decisions to determine eligibility for a clearance. Thus, the total number of days to determine eligibility for a clearance includes investigative time; DISCO and possibly DOHA review time; additional DISCO investigative time, if required; and DOHA's appeals process that may follow the denial of a clearance request or the revocation of a clearance. Finally, the Case Control Management System has the capability to monitor overdue reinvestigations and generate accurate estimates for that portion of the backlog for industry personnel; however, it does not have this capability for military members and federal employees.

We conducted our review from July 2003 through May 2004 in accordance with generally accepted government auditing standards. We include a comprehensive list of related GAO products at the end of this report.

Appendix II: Excerpts from the Adjudicative Guidelines for Determining Eligibility for Access to Classified Information

The Federal Adjudicative Guidelines for Determining Eligibility for Access to Classified Information were approved by the President on March 24, 1997,¹ and implemented by the Department of Defense in 1998. They include the following 13 guidelines and the reasons for concern.

1. *Allegiance to the United States:* The willingness of an individual to safeguard classified information is in doubt if there is any reason to suspect the individual's allegiance to the United States.
2. *Foreign influence:* A security risk may exist when an individual is bound by affection, influence, or obligation to persons, such as family members, who are not citizens of the United States or may be subject to duress.
3. *Foreign preference:* When an individual acts in such a way as to indicate preference for a foreign country, such as possession and/or use of a foreign passport, then he or she may be prone to make decisions harmful to the interests of the United States.
4. *Sexual behavior:* Sexual behavior is a security concern if it involves a criminal offense; indicates a personality or emotional disorder; may subject the individual to undue influence of coercion, exploitation, or duress; or reflects lack of judgment or discretion.
5. *Personal conduct:* Conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, or unwillingness to comply with rules and regulations could indicate that an individual may not properly safeguard classified information.
6. *Financial considerations:* An individual who is financially overextended is at risk of having to engage in illegal acts to generate funds. Unexplained affluence is often linked to proceeds from financially profitable criminal acts.
7. *Alcohol consumption:* Excessive alcohol consumption often leads to the exercise of questionable judgment, unreliability, and failure to control impulses, and increases the risk of unauthorized disclosure of classified information due to carelessness.

¹The White House, "Implementation of Executive Order 12968," Memorandum (Washington, D.C.: Mar. 24, 1997). This memorandum approves the adjudicative guidelines, temporary eligibility standards, and investigative standards required by Executive Order No. 12968, *Access to Classified Information*, Aug. 2, 1995.

8. *Drug involvement*: Improper or illegal involvement with drugs raises questions regarding an individual's willingness or ability to protect classified information.
9. *Emotional, mental, or personality disorders*: Emotional, mental, or personality disorders are a security concern because they may indicate a defect in judgment, reliability, or stability.
10. *Criminal conduct*: A history or pattern of criminal activity creates doubt about a person's judgment, reliability, and trustworthiness.
11. *Security violations*: Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information.
12. *Outside activities*: Involvement in certain types of outside employment or activities is a security concern if it poses a conflict with an individual's security responsibilities and could create an increased risk of unauthorized disclosure of classified information.
13. *Misuse of information technology systems*: Noncompliance with rules, procedures, guidelines, or regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness, and ability to properly protect classified systems, networks, and information.

The guidelines state that each case is to be judged on its own merits and that a final determination to grant, deny, or revoke access to classified information is the responsibility of the specific department or agency. The adjudicators are to consider available, reliable information about the person—past and present, favorable and unfavorable—in reaching an “overall common sense” clearance-eligibility determination that gives careful consideration to the 13 adjudicative guidelines. According to the guidelines, any doubt about whether a clearance for access to classified information is consistent with national security is to be resolved in favor of national security.

Appendix III: Comments from the Department of Defense



OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

May 10, 2004

Mr. Derek B. Stewart, Director
Defense Capabilities and Management
U.S. General Accounting Office
Washington, DC20548

Dear Mr. Stewart:

This is the Department of Defense (DoD) response to the GAO draft report, GAO-04-632, "DOD PERSONNEL CLEARANCES: Additional Steps Can Be Taken to Reduce Backlogs and Delays in Granting Security Clearances to Industry Personnel," dated April 19, 2004 (GAO Code 350522).

As industrial personnel are part of the same clearance process that has resulted in significant delays for government and military personnel the statistics noted in your report are not surprising. What I find of note is that that the number of eligibility determinations for Industry increased by 176% since FY 2001.

There are many significant initiatives underway that are gradually improving the process and there is little acknowledgment of those initiatives in this report. Nor is there any acknowledgement of the policy changes that have been implemented by DoD over the past years to expedite industry's access to classified information.

Since 1986, contractor employees who are found eligible have been automatically issued Interim SECRET clearances within 3 days of their paperwork being received. These employees can then be put to work on classified programs requiring access to SECRET classified information. As acknowledged in the GAO report, reciprocity of security clearances within DoD has not been a problem for DoD personnel and Industry has even been authorized to grant access to employees based on confirmation of a clearance from another contractor or government source.

Industry is now authorized access to the Joint Personnel Adjudication System (JPAS) and will be responsible for maintaining the access records for their own employees. They will also be able to determine the eligibility status of other government, military and contractor personnel to readily facilitate the transfer of the clearances of these personnel.

We have significantly increased the number of adjudicative personnel and instituted process reforms that will expedite the adjudication of contractor investigations. DoD is conducting the research and developing the new automated systems that could



**Appendix III: Comments from the Department
of Defense**

soon revolutionize how investigations are conducted and is working through the interagency process to obtain approval of new investigative standards to leverage the new technologies.

I appreciate the opportunity to comment on the report, but note that this is yet another GAO Report that highlights the bad news while giving passing if any notice to the significant improvements being made. Comments on the specific recommendations are enclosed. Technical comments on the report have been provided under separate cover to the GAO team leader.

Sincerely


for Carol A. Haave
Deputy Under Secretary of Defense
Counterintelligence and Security

Enclosure
As stated

GAO-04-632/GAO CODE 350522

“DOD PERSONNEL CLEARANCES: ADDITIONAL STEPS CAN BE TAKEN TO REDUCE BACKLOGS AND DELAYS IN GRANTING SECURITY CLEARANCES TO INDUSTRY PERSONNEL”

DEPARTMENT OF DEFENSE COMMENTS TO THE RECOMMENDATIONS

Recommendation 1: The GAO recommended that the Secretary of Defense direct the Under Secretary of Defense for Intelligence to improve projections of industrial personnel clearance requirements—both numbers and types of clearances—by working with DoD components, industrial contractors, and the acquisition community to identify obstacles and implement steps to overcome the obstacles. (Page 28/Draft Report)

DoD Response: Concur: While we concur that the process for projecting industrial personnel clearance requirements can be improved, we believe that the current system of surveying cleared contractors annually to obtain best estimates of the number of background investigations required for contract performance has yielded fairly accurate results. Actual submissions in FY01 were 92% of the projection for that year; actual submissions in FY02 were 103% of the projection; and actual submitted in FY03 was 114% of the projection. While the total number of cases being submitted is close to the projection, we are starting to see a change in the mix of cases. During FY03, there was a significant increase in the number of requests for SSBI for initial Top Secret clearances.

	Projected Target for Submission	Actual Submitted	% of Target
FY01			
SSBI	13,450	11,662	87%
TS PR	21,760	16,566	76%
NACLC	78,350	77,113	98%
Other	3,815	2,172	57%
Total	117,375	107,513	92%
FY02			
SSBI	15,033	17,751	118%
TS PR	17,983	23,272	129%
NACLC	101,756	97,419	96%
Other	4,010	4,843	121%
Total	138,782	143,285	103%

Appendix III: Comments from the Department of Defense

<u>FY03</u>			
SSBI	14,419	21,905	152%
TS PR	24,408	23,029	94%
NACLIC	92,395	102,777	111%
Other	2,688	4,348	162%
Total	133,910	152,059	114%
<u>FY04 (at mid-year – thru Mar 31)</u>			
SSBI	28,374	12,939	46%
TS PR	23,017	7,335	32%
NACLIC	117,429	49,001	42%
Other	0	72	
Total	168,820	69,347	41%

A plan is being developed to link the number of investigations required for contract performance to the Contract Security Classification Specification (DD 254), and to require that the number be authorized by the contracting officer. This will allow DSS to better monitor requirements and tie them to the budget process. An electronic DD 254 database with personnel clearance information can be linked to the contract database maintained by the acquisition community, thus tying the clearance process more closely to the acquisition process.

RECOMMENDATION 2: The GAO recommended that the Secretary of Defense direct the Under Secretary of Defense for Intelligence to work with DoD components and other agencies to eliminate unnecessary reciprocity limitations for industry personnel, whose eligibility for a clearance is granted by DoD. (Page 28/Draft Report)

DoD Response: Concur. The Department of Defense assures reciprocity of security clearances through the transfer, reinstatement and conversion policies currently in place and by accepting background investigations and security clearance determinations from all other federal departments for access to equivalent levels and below. Contractors under the NISP already have the authority to transfer clearance eligibility from one company to another and from a government entity to a contractor facility without any action being required by the Department through use of a waiver to the National Industrial Security Program Operating Manual (NISPOM). Industry has been given access to JPAS, which will be the system of record for eligibility and access information for the Department of Defense. As of April 24, 2004 there were 4,377 industry users of JPAS. These users are validating the data contained in the system in preparation for JPAS becoming the system of record for industry as of September 2004. Companies can view a person's eligibility for access, immediately grant collateral access, and are responsible for recording the access into the system. When accesses are terminated, the company is responsible for recording that action, as well.

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.

The Department is participating in several inter-agency reciprocity working groups to identify both the impediments and corrective action to the reciprocity issues between Federal agencies. This office is also working with the SAP community to clearly identify the additional risk determinations required prior to granting access to a specific program and to ensure full reciprocity between programs of “like” risk. Similar processes are underway with the Intelligence Community for the granting of access to SCI.

RECOMMENDATION 3: The GAO recommended that the Secretary of Defense direct the Under Secretary of Defense for Intelligence to develop and implement an integrated, comprehensive management plan to eliminate the backlog, reduce delays in determining eligibility for security clearances, and overcome the impediments that could allow such problems to recur. (Page 28/Draft Report)

DoD Response: Partially Concur. The Department has numerous plans underway to improve the PSI process from “end-to-end.” These plans align changes with functional responsibilities. GAO does not identify why a single, comprehensive, management plan would improve our ability to achieve success.

In November 2002, the Department of Defense made the decision to divest the PSI function and procure these services from OPM. This decision came from the Secretary’s Business Improvement Council under the Senior Executive Council, and is reflected in the President’s Budget for FY 2004. The transfer of PSIs to OPM and the corresponding transformation of DSS is intended to result in the permanent elimination of the investigative and adjudicative backlogs, and reduce delays in determining eligibility for clearances.

The implementation of this effort is quite extensive, and significantly impacts both DSS and OPM. The briefing package “Reengineering Personnel Security” provided to the GAO team represents the high-level plan for the transfer of PSIs to OPM and the corresponding transformation of DSS. A high-level implementation plan is contained in the FY 2004 DSS Performance Plan, which was originally drafted as the implementation plan. A transition team has been in operation since November 2002 administering the details of the implementation. The team has addressed the budget, personnel resources, and costs associated with the transfer and transformation efforts.

The transfer of the DSS investigative workforce will give OPM a federal investigative strength to accomplish the most critical and sensitive investigations. At the same time, OPM will be increasing its contractor base of investigators to ensure sufficient investigative resources for the federal investigative workload. Investigations are a core competency of OPM, so by moving all DoD investigations to OPM and centralizing the contracting function for investigations, capacity will be leveraged, resulting in decreasing investigative timelines.

The collaborative adjudicative support element being established at DoD will provide oversight for DoD investigations and adjudications. This includes oversight of the efforts that are underway to leverage technology to accomplish low risk investigations through data mining and other automated mechanisms. This is intended to decrease the traditional investigative workload, facilitate increased investigative capacity, and result in faster case completion times for the most critical investigations.

The DSS collaborative adjudication support will provide common services for all of the DoD CAFs. Such services will include acquisition and contracting oversight. This DSS organization will also leverage DSS' relationship with industry as the single Industry CAF for all industry clearances, including interim, suitability and trustworthiness determinations. The adjudicative process will cover SCI accesses. These efforts are intended to streamline the DoD adjudicative process, facilitating faster adjudicative timelines.

RECOMMENDATION 4: The GAO recommended that the Secretary of Defense direct the Under Secretary for Intelligence to analyze the feasibility of implementing initiatives designed to reduce the backlog and delays, prioritize the initiatives, and make resources available for testing and implementing the initiatives, which could include, but are not limited to, those evaluated in this report. (Page 28/Draft Report)

DoD Response: Concur. Ongoing actions specific to each of the GAO evaluated initiatives are identified below:

- **Phased Periodic Reinvestigation (PR):**

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 (PERSEREC) 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) on May 3, 2004. 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.

- **Industry Central Adjudication Facility (CAF):**

One of the key ongoing initiatives to improve PSI processing for industry is to expand the DISCO adjudicative role to serve as the nucleus for a single central adjudication facility

(CAF) that will handle all adjudications for Industry, to include trustworthiness and SCI determinations. This plan, including the proposed structure, authorities, training and resource details, should be finalized this calendar year. DISCO has instituted a process to adjudicate Industry cases up to the statement of reasons (SOR). Should DISCO believe an SOR is required, the case is referred to DOHA for further evaluation and issuance of the SOR if DOHA determines it to be appropriate.

- Evaluation of investigative and adjudicative standards

The Department is currently participating with other Federal agencies in an evaluation of the utility and effectiveness of the current security background investigations and security clearance procedures of the federal government. When that evaluation is completed, a copy will be provided to the GAO.

- Requirements-identification improvements

As part of the automation of the Contract Security Classification Specification (DD 254), the contracting officer and the contractor will determine the number of investigations required for contract performance. When a contractor investigative request is received in JPAS it will be validated against this contract database to verify the need for the investigation. This will allow DSS to better monitor investigative requirements and tie the requirements to the budget process. The requirements definition phase is currently underway for this initiative.

- 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, specified databases are 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 automatically identifies and schedules cleared personnel for a series of database checks that include: credit reports, FBI criminal history, Treasury large currency transaction filings, Customs foreign travel, and real estate ownership records. The report produced by the database will be electronically forwarded to each 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 cycles 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.

Related GAO Products

DOD Personnel Clearances: Preliminary Observations Related to Backlogs and Delays in Determining Security Clearance Eligibility for Industry Personnel. [GAO-04-202T](#). Washington, D.C.: May 6, 2004.

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.

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

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.

Related GAO Products

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.

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