United States Government Accountability Office

Report to Congressional Requesters

January 2024

FEDERAL WORKFORCE

Actions Needed to Improve the Transfer of Personnel Security Clearances and Other Vetting Determinations

Accessible Version

GAO-24-105669

GAO Highlights

Highlights of GAO-24-105669, a report to congressional requesters

January 2024

FEDERAL WORKFORCE

Actions Needed to Improve the Transfer of Personnel Security Clearances and Other Vetting Determinations

Why GAO Did This Study

Personnel vetting processes help ensure the trustworthiness of the federal government's workforce. Federal agencies vet personnel to determine whether they are suitable for employment or eligible to access classified information, among other things. Agencies are generally required to accept personnel vetting determinations that other agencies have previously made. This reciprocity can promote personnel mobility and help reduce skills gaps.

GAO was asked to review personnel vetting reciprocity issues. This report assesses the extent to which ODNI and OPM have (1) collected reliable data on agency reciprocity in the personnel vetting processes and (2) addressed reciprocity challenges that agencies and contractors face.

GAO analyzed ODNI data on reciprocity for fiscal years 2019 through 2021, and data from five agencies selected to obtain a diverse set of perspectives. GAO also surveyed a nongeneralizable sample of 31 agencies and 600 contractors (293 responded).

What GAO Recommends

GAO made eight recommendations to ODNI and OPM, including that ODNI follow best practices to evaluate the reliability of data, ODNI and OPM develop and implement a plan to ensure that IT systems contain complete and accurate information, and ODNI develop and implement a plan to inform contractors about the status of reciprocity determinations. OPM concurred with the recommendations directed to it. ODNI did not provide formal comments on the recommendations.

View GAO-24-105669. For more information, contact Alissa H. Czyz at (202) 512-3058 or czyza@gao.gov.

What GAO Found

The Office of the Director of National Intelligence (ODNI) and the Office of Personnel Management (OPM)—two agencies with key personnel vetting oversight responsibilities—do not have reliable data on the extent to which agencies have honored previously granted vetting determinations, known as reciprocity. GAO found that reciprocity data ODNI collected from agencies were inconsistent and incomplete, as described below.

- **Data were inconsistent.** Agencies sometimes reported data to ODNI by component and other times at the agency level, according to ODNI officials. For example, in fiscal year 2019, the Treasury Department reported data by each of its components for the first two quarters but reported data at the department level in the third quarter, according to ODNI officials.
- **Data were incomplete.** Two of five agencies GAO analyzed did not report required data to ODNI on the frequency with which they determined individuals were ineligible for reciprocity. ODNI officials said they did not know how many agencies should report data to them, but have initiated an assessment to do so.

By following best practices for evaluating the reliability of data—such as tracing a sample of data records to or from source documents to assess the accuracy and completeness of the data—ODNI could improve its oversight of security clearance reciprocity.

ODNI and OPM have not fully addressed all reciprocity-related challenges that agencies and contractors face (see figure). For example, 28 of the 31 agencies GAO surveyed stated that information technology (IT) systems at times did not have complete information needed to make reciprocity determinations. If ODNI and OPM took actions to mitigate this and other challenges, agencies may be able to grant reciprocity more often and more quickly.

Reciprocity Challenges That Agencies and Contractors Face

Source: GAO analysis of agency documentation, survey results, and interviews; GAO (design). | GAO-24-105669

Contractors reported that agencies did not provide updates when the security clearance reciprocity process was delayed. If ODNI develops and implements a plan to ensure that contractors are informed about the status of reciprocity determinations, contractors may be able to plan projects and hire personnel better, which could have positive effects on government contracts.

Contents

Abbreviations

CVS	Central Verification System
DCSA	Defense Counterintelligence and Security Agency
DOD	Department of Defense
FPDS	Federal Procurement Data System
IC	intelligence community
IT	information technology
NBIS	National Background Investigation Services
ODNI	Office of the Director of National Intelligence
OPM	Office of Personnel Management
PAC	Performance Accountability Council
SCIF	Sensitive Compartmented Information Facility
SEAD	Security Executive Agent Directive

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

January 22, 2024

The Honorable Jamie Raskin
Ranking Member
Committee on Oversight and Accountability
House of Representatives

The Honorable Gerald E. Connolly
House of Representatives

Personnel vetting processes help ensure the trustworthiness of the federal government's workforce. Among other things, vetting helps prevent unauthorized disclosure of classified information to foreign intelligence services or other actors. Specifically, federal departments and agencies vet personnel to determine whether they are (1) eligible to access classified information or to hold a sensitive position, (2) suitable for government employment or fit to perform work for, or on behalf of, the government as contractor employees or certain categories of federal employees, and (3) eligible for access to agency systems or facilities.[1]

In addition, departments and agencies are required to recognize and accept personnel vetting background investigations and adjudications that other departments and agencies have previously made (hereafter

[1]The term *fitness* is defined in Executive Order 13,488 as the level of character and conduct determined necessary for an individual to perform work for or on behalf of a federal agency as an employee in the excepted service (other than a position subject to suitability) or as a contractor or nonappropriated fund employee. Exec. Order No. 13,488, *Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust*, § 2(d), *as amended through* Exec. Order No. 13,764, *Amending the Civil Service Rules, Executive Order 13488, and Executive Order 13467 to Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters*, 82 Fed. Reg. 8,115 (Jan. 17, 2017).

referred to as reciprocity), with certain exceptions.[2] Effectively transferring personnel vetting determinations from one department or agency to another is key to enabling personnel mobility across the federal government.[3] For example, personnel mobility can help agencies access personnel with the skills needed to accomplish their missions. In the 2023 update to our high-risk series, we reported that mission-critical skills gaps specific to federal agencies and across the federal workforce pose a high risk to the nation. Enabling personnel mobility is one way to help close those skills gaps.[4]

The Director of National Intelligence is the federal government's Security Executive Agent. In this role, the director is responsible for the development and issuance of uniform and consistent policies and procedures to ensure the effective, efficient, timely, and secure completion of investigations as well as determinations for eligibility for access to classified information or eligibility to hold a sensitive position. The responsibilities of the Director of National Intelligence as the Security Executive Agent extend beyond the intelligence community (IC) to cover government-wide personnel security processes, including ensuring

[2]See Exec. Order No. 13,467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*, § 2.2, *as amended through* Exec. Order No. 13,869, *Transferring Responsibility for Background Investigations to the Department of Defense*, 84 Fed. Reg. 18,125 (Apr. 24, 2019). The original Executive Order 13,467 was issued in 2008 and amended several times. For purposes of this report, unless indicated otherwise, Executive Order 13,467, *as amended*, refers to the most recent version of Executive Order 13,467 *as amended* through Executive Order 13,869 in 2019. Specifically, Executive Order 13,467, *as amended*, states except as otherwise authorized by law or policy issued by the applicable Executive Agent, agencies shall accept background investigations and adjudications conducted by other authorized agencies unless an agency determines that a particular background investigation or adjudication does not sufficiently address the standards used by that agency in determining the fitness of its excepted service employees who cannot be noncompetitively converted to the competitive service.

[3]For the remainder of this report, we use the term *agencies* to refer to both executive branch departments and agencies where appropriate. Additionally, for the remainder of the report, we use the term determination to refer to adjudication as defined in Executive Order 13,467, *as amended*. Per this definition, adjudication is the evaluation of pertinent data in a background investigation, as well as any other available information that is relevant and reliable, to determine whether a covered individual is: (i) suitable for government employment; (ii) eligible for logical and physical access; (iii) eligible for access to classified information; (iv) eligible to hold a sensitive position; or (v) fit to perform work for or on behalf of the government as a federal employee, contractor, or nonappropriated fund employee.

[4]GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, GAO-23-106203 (Washington, D.C.: Apr. 20, 2023).

reciprocity for security clearance determinations.[5] The Director of the Office of Personnel Management (OPM), as the federal government's Suitability and Credentialing Executive Agent, has oversight responsibilities for the suitability, fitness, and credentialing processes, including promoting reciprocity of suitability and fitness determinations.[6]

We have previously reported on challenges related to personnel vetting. In 2018, we placed the issue of the government-wide personnel security clearance process on our High-Risk List due to delays with the clearance process, a lack of measures to determine the quality of investigations, and issues with relevant information technology (IT) systems supporting personnel vetting. In April 2023, we noted that progress had been made in reforming the personnel security clearance process, but challenges remained.[7] These included that the Office of the Director of National Intelligence (ODNI) did not have reliable data to assess the extent to which agencies had met goals for the timeliness of the process, that ODNI continued to lack performance measures, and that the Department of Defense (DOD) did not have a reliable schedule to manage the development of a new IT system for personnel vetting.[8]

You asked that we review issues related to agencies granting reciprocity for personnel vetting determinations. In this report, we evaluate the extent to which ODNI and OPM have (1) collected reliable data on agency reciprocity in personnel vetting processes, and (2) addressed challenges

[5]Exec. Order No. 13,467, *as amended*, states that the Director of National Intelligence shall, among other things, ensure reciprocal recognition of eligibility for access to classified information or eligibility to hold a sensitive position among the agencies, including acting as the final authority to arbitrate and resolve disputes among the agencies involving the reciprocity of investigations and determinations of eligibility.

[6]See Exec. Order No. 13,467, § 2.5(b), (c), *as amended*. Specifically, Exec. Order No. 13,467, *as amended*, states that the Director of OPM shall promote reciprocal recognition of suitability or fitness determinations among the agencies, including acting as the final authority to arbitrate and resolve disputes among the agencies involving the reciprocity of investigations and adjudications of suitability and fitness.

[7]For the purposes of this report, we use the term *security clearance process* to refer to the process to determine eligibility for access to classified information or eligibility to hold a sensitive position. In addition, part 731 of title 5, Code of Federal Regulations, defines a suitability determination as a decision by the Office of Personnel Management (OPM) or an agency with delegated authority that a person is suitable or is not suitable for employment in covered positions in the federal government or a specific federal agency. 5 C.F.R. § 731.101 (2023).

[8]GAO-23-106203.

that agencies and contractors face in the personnel vetting reciprocity processes.[9]

For our first objective, we analyzed the reliability of data that ODNI and OPM collect and use to oversee the extent to which agencies grant reciprocity for personnel vetting determinations. We also reviewed key documents, including a 2021 audit report on security clearance reciprocity prepared by the Intelligence Community Inspector General.[10] We also analyzed data that a nongeneralizable selection of five agencies submitted to ODNI and interviewed officials from these agencies about their data collection.

We selected these agencies from various sectors of the executive branch including defense, intelligence, and nondefense and nonintelligence. We also considered the number of employees in the department or agency and whether they had the authority to conduct background investigations, according to ODNI. The five agencies we selected are: the U.S. Agency for International Development, the Drug Enforcement Administration, the Defense Counterintelligence and Security Agency (DCSA), the Defense Intelligence Agency, and the Department of Veterans Affairs.

In addition, we compared ODNI actions related to data on reciprocity for security clearances to principles established in *Standards for Internal Control in the Federal Government* related to management's use of quality information to achieve its objectives.[11] Further, we compared OPM actions related to data on reciprocity for suitability, fitness, and credentialing determinations to best practices we established in a guide on assessing the reliability of data.[12] We found that ODNI's and OPM's data were not sufficiently reliable to determine the extent that agencies granted reciprocity for personnel vetting determinations. We describe these issues in more detail later in this report.

[9]We use the term contractor here and elsewhere in this report to refer to private organizations performing on contracts with the federal government.

[10]Office of the Intelligence Community Inspector General, *Final Report: Evaluation of Intelligence Community Implementation of Security Clearance Reciprocity*, INS-2020-001 (Washington, D.C.: Oct. 6, 2021).

[11]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 10, 2014).

[12]GAO, *Assessing Data Reliability*, GAO-20-283G (Washington, D.C.: Dec. 16, 2019).

For our second objective, we obtained information about reciprocity-related challenges agencies and contractors face by interviewing officials from agencies including ODNI, OPM, and DOD. We also interviewed officials within private organizations that perform contracting work for the federal government. We reviewed relevant documentation on these challenges. We then selected and surveyed a nongeneralizable sample of 31 agencies from a universe of 83 agencies in four categories: cabinet-level departments, large and medium-sized independent agencies, and IC elements. We also selected a random, nongeneralizable sample of 600 contractors to better understand their reciprocity-related challenges.

For our agency survey, we requested that agencies complete one survey that reflected the organizational perspective, and all 31 agencies provided responses. For our contractor survey, we surveyed one security official within each organization and asked them to confirm that they had experience requesting agencies to grant reciprocity for contractor employees from 2019 through 2021. We received responses from 293 contractors. Although our samples are nongeneralizable, the information obtained from these agencies and contractors offer useful insights and perspectives on reciprocity challenges and ways to address them. Next, we analyzed the responses to our surveys, which included conducting content analysis of responses to open-ended questions. Additionally, we interviewed officials from ODNI, OPM, DOD, and the five selected agencies previously described.

We compared challenges that ODNI, OPM, and survey respondents identified to requirements that the Director of National Intelligence established for security clearance reciprocity in Security Executive Agent Directive 7 (SEAD 7),[13] and principles established in the *Standards for Internal Control in the Federal Government*.[14] Further information on our scope and methodology can be found in appendix I.

[13]ODNI, SEAD 7, *Reciprocity of Background Investigations and National Security Adjudications* (Nov. 9, 2018) establishes requirements for reciprocal acceptance of background investigations and determinations for initial or continued eligibility for access to classified information or eligibility to hold a sensitive position. SEAD 7 requires agencies to accept background investigations completed by an authorized investigative agency that meet all or part of the investigative requirements for a security clearance background investigation with some exceptions, such as when new information of adjudicative relevance has been reported, developed, or known to agency officials or the most recent background investigation is more than 7 years old.

[14]GAO-14-704G.

We conducted this performance audit from January 2022 to January 2024 in accordance with generally accepted government auditing standards.[15] Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Governance Structure for Personnel Vetting Reform and Reciprocity

In June 2008, Executive Order 13,467 established the Security, Suitability, and Credentialing Performance Accountability Council (PAC) as the government-wide entity responsible for implementation of reforms to the federal government's personnel vetting processes.[16] The executive order, as amended, outlines the responsibilities of the PAC, designates the four principal members of the PAC, and specifies the responsibilities of the principal members, including responsibilities for reciprocity (see table 1).[17]

[15]Our time frames for completing our review were affected, in part, by delays in obtaining needed information.

[16]See Exec. Order No. 13,467, § 2.2(a), (c)-(d), 73 Fed. Reg. 38,103, 38,105 (June 30, 2008). The PAC was originally established as the Suitability and Security Clearance Performance Accountability Council; its name was updated in 2017.

[17]See Exec. Order No. 13,467, *as amended*.

Table 1: The Performance Accountability Council (PAC) Principal Members and Responsibilities Related to Reciprocity as Outlined in Executive Order 13,467, as amended

PAC principal member	Role of the PAC and responsibilities related to reciprocity
The Deputy Director for Management of the Office of Management and Budget[a]	Shall serve as chair of the PAC. Facilitates, consistent with the executive branch's enterprise strategy, adoption of enterprise-wide standards and solutions to ensure security, quality, reciprocity, efficiency, effectiveness, and timeliness.
The Director of National Intelligence[b]	Shall serve as the Security Executive Agent. May issue guidelines and instructions to the heads of agencies to ensure appropriate uniformity, centralization, efficiency, effectiveness, timeliness, and security in processes relating to determinations by agencies of eligibility for access to classified information or eligibility to hold a sensitive position, to include such matters as investigations, polygraphs, adjudications, and reciprocity. Shall ensure the reciprocal recognition of eligibility to access classified information or to hold a sensitive position among the agencies.
The Director of the Office of Personnel Management[c]	Shall serve as the Suitability and Credentialing Executive Agent. May issue guidelines and instructions to the heads of agencies to promote appropriate uniformity, centralization, efficiency, effectiveness, reciprocity, timeliness, and security in processes relating to determining suitability or fitness. May develop guidelines and instructions for the heads of agencies as necessary to ensure appropriate uniformity, centralization, efficiency, effectiveness, and timeliness in processes relating to eligibility for a personal identity verification credential. Shall promote reciprocal recognition of suitability or fitness determinations among the agencies.
The Under Secretary of Defense for Intelligence and Security[d]	Shall serve as a Principal Member of the PAC. Also, Executive Order 13,467 directs the Secretary of Defense to (1) design, develop, deploy, operate, secure, defend, and continuously update and modernize, as necessary, the information technology systems that support all personnel vetting processes conducted by the Department of Defense and (2) establish the Defense Counterintelligence and Security Agency to serve as the primary federal entity for conducting background investigations for the federal government.[e]

Source: Executive Order 13,467, *as amended*. | GAO-24-105669

[a]Exec. Order No. 13,467, § 2.4(b), (e), *as amended*.

[b]Exec. Order No. 13,467, § 2.5(e), *as amended*.

[c]Exec. Order No. 13,467, § 2.5(b), (c), *as amended*.

[d]Exec. Order No. 13,467, § 2.4(b), *as amended*.

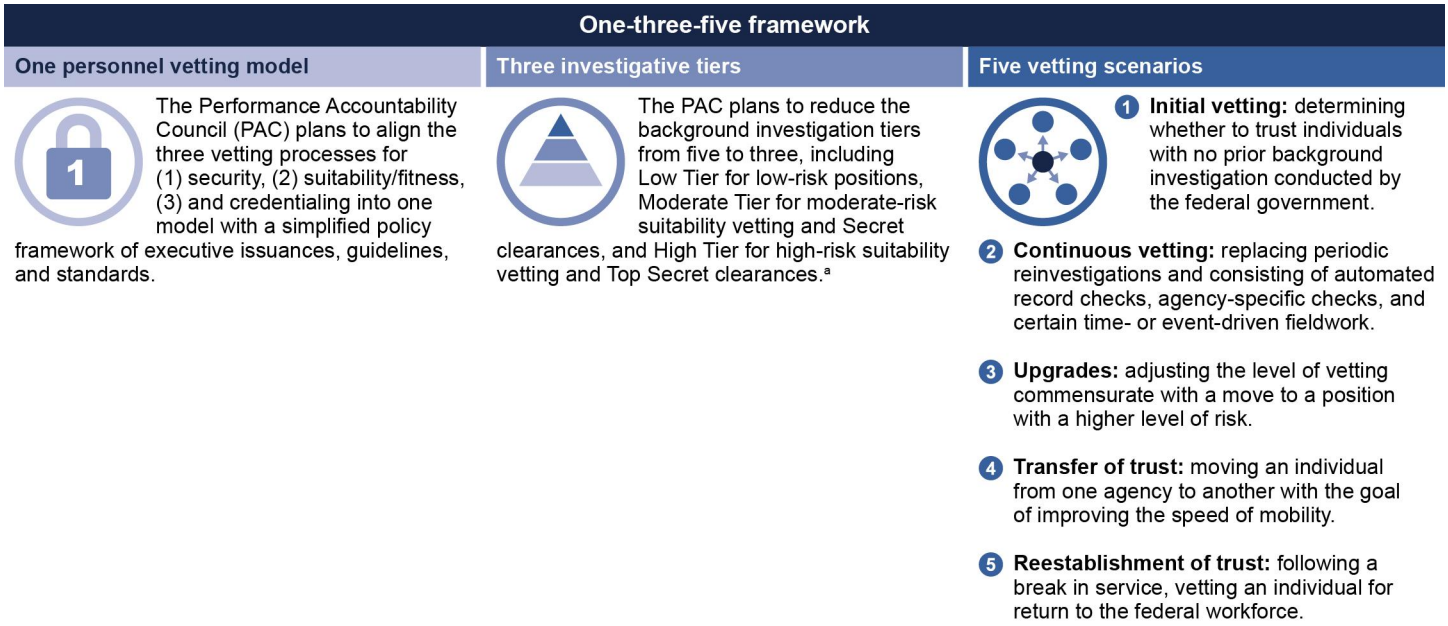
[e]Specifically, the executive order directed the Secretary of Defense to rename the Defense Security Service as the Defense Counterintelligence and Security Agency. Exec. Order No. 13,467, § 2.6(b), as amended.

Moreover, in April 2014, the PAC established a Program Management Office to implement personnel security clearance reforms. This office is staffed with subject-matter experts with knowledge of personnel security clearances and suitability determinations from the Office of Management and Budget, OPM, DOD, the Department of Homeland Security, the Department of Justice, the Department of the Treasury, and the Federal Bureau of Investigation.

Trusted Workforce 2.0

In March 2018, the PAC's principal members initiated Trusted Workforce 2.0 to reform the personnel vetting processes. The PAC issued the Trusted Workforce 2.0 Implementation Strategy in April 2022, which states that the reform aims to better support agencies' missions by reducing the time required to bring new hires onboard, enabling mobility of the federal workforce, and improving insight into workforce behaviors. This strategy is updated on a quarterly basis in coordination with stakeholder agencies to ensure it reflects current progress and addresses emerging priorities, according to officials from the Office of Management and Budget. The PAC is incrementally implementing Trusted Workforce 2.0 and plans to fully implement the reform in fiscal year 2026.[18] The reform's "one-three-five" framework is depicted and explained in figure 1.

Figure 1: Trusted Workforce 2.0 Framework



Source: PAC documentation; GAO (design). | GAO-24-105669

Note: Under Trusted Workforce 2.0, "transfer of trust" is the term used to refer to reciprocity for personnel vetting determinations.

[18]For example, according to the *Personnel Vetting Quarterly Progress Update* for the third quarter of fiscal year 2023, the PAC anticipates that agencies will complete the enrollment of all populations into continuous vetting programs by March 2026.

[a]The three investigative tiers will include: Low Tier for low-risk non-sensitive positions and physical or logical access or credentialing determinations; Moderate Tier for moderate-risk public trust and noncritical sensitive positions and granting eligibility and access to classified information at the Confidential or Secret level, or L access; and High Tier for high-risk public trust and critical or special sensitive positions and granting eligibility and access to classified information at the Top Secret level, access to sensitive compartmented information, or Q access. See Director of National Intelligence and Director, OPM, Federal Personnel Vetting Investigative Standards (May 17, 2022).

Scope of Personnel Vetting and Reciprocity Processes

Under Executive Order 13,467, personnel who perform, or seek to perform, work for, or on behalf of the executive branch—including federal employees, military members, or contractor personnel—are required to undergo a background investigation. The purpose of the investigation is to determine whether they are suitable or fit for government employment or fit to perform work for, or on behalf of, the government as contractor employees or nonappropriated fund employees.[19] In addition, such personnel where relevant are also required to undergo background investigations to determine if they are eligible for a personal identity verification credential permitting logical and physical access to federally controlled information systems and federally controlled facilities.[20] Further, such personnel where relevant are required to undergo background investigations to determine if they are eligible to access classified information or to hold a sensitive position.[21] Afterward, the relevant agency evaluates pertinent data from the background investigation, as well as any other available information that is relevant and reliable, to

[19]See Exec. Order No. 13,467, § 1.3(h), (l), *as amended*.

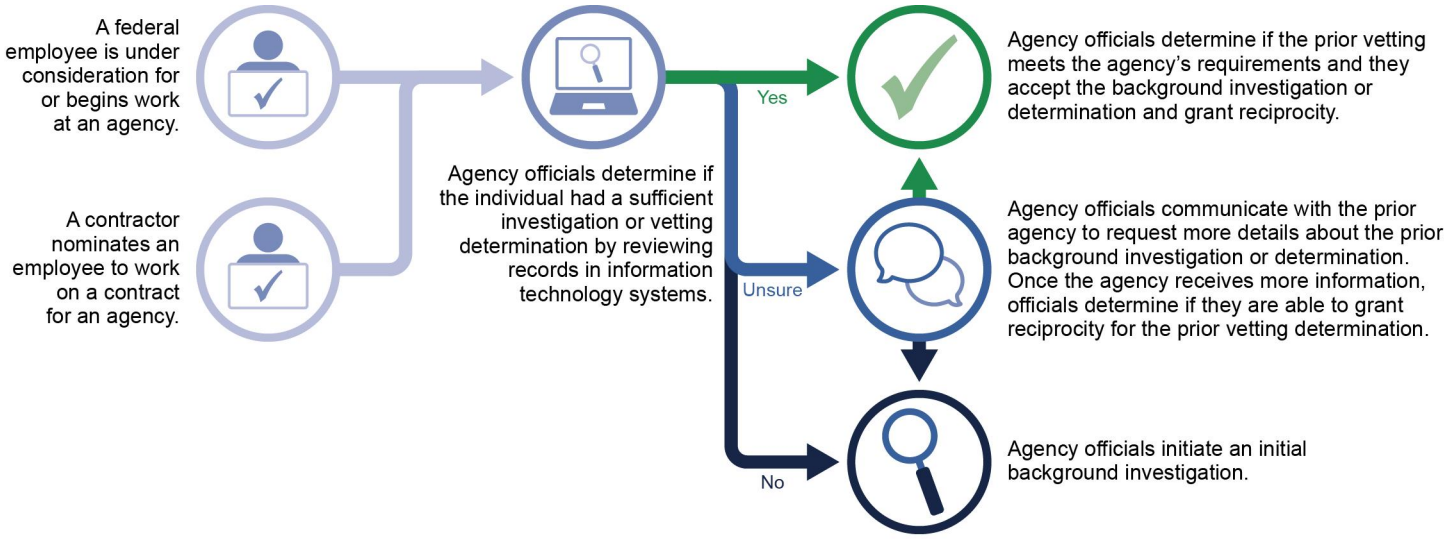
[20]See Exec. Order No. 13,467, § 1.3(h), (l), (m), *as amended*. Logical access control systems control an individual's ability to access one or more computer system resources such as a workstation, network, application, or database. A logical access control system requires validation of an individual's identity through some mechanism such as a personal identification number, card, biometric, or other token. It has the capability to assign different access privileges to different persons depending on their roles and responsibilities in an organization. Committee on National Security Systems Instruction 4009, *Committee on National Security Systems (CNSS) Glossary* (Mar. 2, 2022).

[21]See Exec. Order No. 13,467, § 1.3(h), (l), *as amended*. The order defines classified information as information that has been determined pursuant to Executive Order 13,526, *Classified National Security Information*, 75 Fed. Reg. 707, 707-731 (Dec. 29, 2009), or a successor or predecessor order, or the Atomic Energy Act of 1954, to require protection against unauthorized disclosure. It defines a sensitive position as any position within or in support of a department or agency, the occupant of which could bring about, by virtue of the nature of the position, a material adverse effect on the national security, regardless of whether the occupant has access to classified information, and regardless of whether the occupant is an employee, a military service member, or a contractor.

make a determination for the individual in one or more of these personnel vetting categories.

To grant reciprocity for a personnel vetting determination, agency officials review records in government-wide IT systems (these are described below). Officials review the status of an individual's background investigation and eligibility determination to assess whether the individual is eligible for reciprocity. According to ODNI officials, agency personnel often make two separate reciprocity decisions: one for suitability or fitness and a second for a security clearance, each with different standards and potentially differing outcomes. See figure 2 for the process that agency officials use when considering whether to grant reciprocity for a background investigation or personnel vetting determination made by another agency.

Figure 2: Process for Considering Whether to Grant Reciprocity for Background Investigations or Personnel Vetting Determinations



Source: GAO analysis of agency documentation and interviews; GAO (design). | GAO-24-105669

Note: Additional steps may be involved for national security determinations involving polygraphs.

IT Systems for Reciprocity Determinations

To make reciprocity determinations, agency officials review records in one or more of three IT systems to determine whether an individual has had a prior background investigation or vetting determination that meets the agency's needs. The three IT systems are the Central Verification

System (CVS), the Defense Information System for Security, and Scattered Castles.

- CVS is the primary IT system non-DOD agencies use to make reciprocity determinations. CVS contains information on investigations and determinations for security clearances, eligibility to hold a sensitive position, and suitability, fitness, and credentialing determinations for personnel from most agencies. DCSA is responsible for maintaining CVS.
- Defense Information System for Security is the IT system that DOD officials use to make reciprocity determinations. It contains records for security clearances; eligibility to hold a sensitive position; and suitability, fitness, and credentialing determinations for DOD military personnel, civilians, and contractor personnel.
- Scattered Castles is the IT system that IC personnel use to make reciprocity determinations. It contains information about security clearances and eligibility to hold a sensitive position for IC personnel as well as information about personnel from agencies that are not IC elements.

Since 2016, DOD has been developing a new IT system called the National Background Investigation Services (NBIS) to manage the end-to-end personnel vetting processes, including reciprocity, for most of the federal workforce. DOD plans, for the future, that NBIS will replace CVS and the Defense Information System for Security. However, in 2021, we reported that DCSA—which is responsible for developing and implementing NBIS—did not have a reliable schedule to manage NBIS.[22] We recommended that DCSA revise the NBIS schedule to fully meet the characteristics of a reliable schedule, and DOD concurred with our recommendation.

However, in August 2023, we reported that DCSA still did not have a reliable schedule for NBIS. We also found that DCSA may not be able to

[22]GAO, *Personnel Vetting: Actions Needed to Implement Reforms, Address Challenges, and Improve Planning*, GAO-22-104093 (Washington, D.C.: Dec. 9, 2021). In addition to developing NBIS, DCSA conducts the majority of background investigations for the executive branch. The executive branch transferred the responsibility for the government-wide background investigation mission from OPM to DOD as of October 1, 2019. While DCSA conducts the majority of background investigations, some agencies have the authority to conduct all or some of their own investigations. These agencies are investigative service providers and, according to ODNI, include the Central Intelligence Agency, the Federal Bureau of Investigation, and the State Department. In addition, some DOD components, including the National Security Agency, have the authority to conduct their own investigations, according to ODNI.

accurately project NBIS costs because its 2022 cost estimate was not reliable. We suggested that Congress consider requiring DCSA to revise its schedule and cost estimates to meet our best practices.[23]

ODNI and OPM Have Not Collected Reliable Data on Reciprocity in the Personnel Vetting Processes

ODNI Has Collected Security Clearance Reciprocity Data, but the Data Are Not Reliable

On a quarterly basis, ODNI requires agencies that conduct personnel vetting for national security positions to report data on the frequency with which they made reciprocity decisions, the time to make each decision, the results of the decisions, and the reasons they denied reciprocity.[24] ODNI uses these data to oversee agencies' reciprocity processes, according to ODNI officials. However, we found that the data ODNI uses to carry out this oversight are unreliable for several reasons:

- **Agencies reported data inconsistently to ODNI**. ODNI officials told us that some agencies at times reported data by component for some quarters but in other quarters, agencies combined the data from components and then reported the data at the agency level. For example, ODNI officials told us that in fiscal year 2019, the Treasury Department reported data by each of its components for the first two quarters but began reporting data at the department level in the third quarter. Similarly, the Department of the Interior provided data at the department level in fiscal year 2020 but at the component level in fiscal year 2021. When agencies report data inconsistently, ODNI is not able to observe trends in the data over time. In July 2023, ODNI

[23]GAO, *Personnel Vetting: DOD Needs a Reliable Schedule and Cost Estimate for the National Background Investigation Services Program*, GAO-23-105670 (Washington, D.C.: Aug. 17, 2023).

[24]DNI Memorandum, *Metrics Reporting Requirements for National Security Vetting in Fiscal Year 2018 and Beyond* (Nov. 19, 2018); Director of the National Counterintelligence and Security Center Memorandum, *Metrics Reporting Requirements for National Security Vetting in Fiscal Year 2018 and Beyond* (Jan. 18, 2019). The National Counterintelligence and Security Center Director's memorandum required the heads of agencies that conduct national security vetting to report data quarterly to ODNI on security clearance topics, including reciprocity.

officials told us that they communicated with agencies to emphasize the importance of submitting consistent data.

- **ODNI did not maintain all the data it collected from agencies**. In August 2022, ODNI provided a data set showing that 16 agencies reported data on reciprocity for fiscal year 2019. However, in June 2023, ODNI officials told us that they had found data from additional agencies for fiscal year 2019 and provided data showing that 43 agencies reported data, raising questions as to whether ODNI has effectively maintained the data it has collected from agencies.
- **ODNI data were incomplete**. Some agencies did not report all required data to ODNI. Specifically, our analysis of data on security clearance reciprocity from the five selected agencies found that DCSA and the Defense Intelligence Agency did not report the required data on the instances that they determined an individual was ineligible for reciprocity and the respective reasons in such instances.[25] Our analysis of data from the Drug Enforcement Administration, the U.S. Agency for International Development, and the Department of Veterans Affairs showed that they submitted the required data to ODNI.
- **ODNI did not have a complete list of all agencies required to report data**. ODNI officials acknowledged that they did not have a complete list of all agencies that conduct vetting for personnel for national security positions and are thus required to report data. They said, as a result, that their data may be incomplete. A 2019 memorandum from an ODNI component—the National Counterintelligence and Security Center—states that ODNI planned to collect data from more than 115 agencies for fiscal year 2019.[26] However, ODNI officials told us that they collected data from about 90 agencies from fiscal years 2019 through 2021. They could not explain why the 2019 memorandum referred to 115 agencies.[27] In June 2023,

[25]DCSA officials told us that they did not provide these data because the Defense Information System for Security does not have the capability to record this information. However, these officials told us in June 2023 that they began recording this information manually and plan to report it to ODNI. Similarly, Defense Intelligence Agency officials acknowledged that they did not provide these data and said their agency's IT system was a contributing factor because it was designed about a decade ago before the Director of National Intelligence established the reporting requirements.

[26]Director of the National Counterintelligence and Security Center Memorandum, *Metrics Reporting Requirements for National Security Vetting in Fiscal Year 2018 and Beyond* (Jan. 18, 2019).

[27]Specifically, ODNI officials told us that 90 agencies reported data on at least one security clearance topic in at least 1 year from fiscal years 2019 through 2021.

ODNI officials told us that they began an assessment to identify all agencies that conduct national security vetting in response to our observations and that they were nearly finished with that assessment.[28]

- **ODNI did not know the number of agencies that had no cases of reciprocity to report**. According to ODNI, some agencies reported data on other security clearance topics but did not report whether they made reciprocity decisions. ODNI interpreted these instances to mean that such agencies made no reciprocity decisions. However, ODNI did not include instructions in the data collection tool requiring agencies to affirm that they had no cases of reciprocity to report. ODNI officials acknowledged that agencies not reporting reciprocity data may have overlooked that part of the data collection tool and that these omissions do not necessarily mean these agencies had no reciprocity decisions to report. Subsequently, ODNI officials told us that, in response to our observations, they plan to update the instructions in the data collection tool to direct agencies to affirm that they have no instances of reciprocity to report when applicable.

NBIS, when fully deployed, may improve the reliability of some reciprocity data for agencies that plan to use it. ODNI officials told us that, under their existing system, agencies transfer data from their internal IT systems to spreadsheets and email those spreadsheets to ODNI. ODNI officials told us that this approach is vulnerable to human error. DCSA plans to incorporate a capability into NBIS that will enable adjudicators to record the data about reciprocity decisions in NBIS. ODNI will then be able to access agency data directly from the system, according to DCSA officials. The officials said that this capability will provide an automated method for ODNI to collect data from agencies and may improve the reliability of the data.

[28]Similarly, the Office of the Inspector General of the Intelligence Community reported in October 2021 that ODNI data from parts of fiscal years 2019 and 2020 on reciprocity for Top Secret cleared and Sensitive Compartmented Information-briefed government personnel from eight IC elements were not always complete and sometimes contained inaccuracies. For example, the Inspector General reported that the Central Intelligence Agency reported data to ODNI on its and ODNI's contractors but did not include data about its government employees. The Inspector General recommended that the Director of the National Counterintelligence and Security Center ensure reciprocity data it receives from data calls is complete and accurate. In July 2023, a senior official from the Office of the Inspector General of the Intelligence Community told us that this recommendation was closed. See Office of the Inspector General of the Intelligence Community, *Final Report: Evaluation of Intelligence Community Implementation of Security Clearance Reciprocity*, INS-2020-001 (Washington, D.C.: Oct. 6, 2021).

In August 2023, we reported that DCSA planned for NBIS to reach full implementation by the end of 2024 but lacked a reliable schedule.[29] However, ODNI officials said that IC elements do not plan to use NBIS due to security and IT challenges related to accessing and using the system. Thus, the data challenges outlined above will likely continue for IC elements and other agencies that do not use NBIS.

Standards for Internal Control in the Federal Government state that agencies' management should use quality information to achieve their objectives.[30] Specifically, according to the standards, management obtains data from reliable sources that are reasonably free from error and bias and evaluates the sources of data for reliability. ODNI officials told us they assess the reliability of the data they collect from agencies by looking for anomalies and trends in the data, running automated calculations, and communicating with agencies about discrepancies. However, officials from DCSA and the Defense Intelligence Agency told us that ODNI officials did not provide any feedback about their data. Nevertheless, they provided incomplete data to ODNI.[31]

ODNI has not collected reliable data because it has not followed best practices for evaluating the reliability of data that agencies submit.[32] These best practices include:

- interviewing knowledgeable officials about their data systems to consider whether data are generated automatically or entered manually and how data are verified,
- reviewing data system documentation such as user manuals and data dictionaries to determine if data entry controls are sufficient to minimize errors, and

[29]GAO-23-105670.

[30]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: September 2014).

[31]Similarly, the 2021 review by the Office of the Inspector General of the Intelligence Community also found that ODNI did not provide feedback to the IC elements in its review about incomplete and inaccurate data. See Office of the Inspector General of the Intelligence Community, *Final Report: Evaluation of Intelligence Community Implementation of Security Clearance Reciprocity*, INS-2020-001 (Washington, D.C.: Oct. 6, 2021).

[32]GAO, *Assessing Data Reliability*, GAO-20-283G (Washington, D.C.: December 2019).

- tracing a sample of data records to or from source documents to assess the accuracy and completeness of the data.

Although ODNI officials told us that they do not use best practices to guide their data collection efforts, they said they are willing to consider doing so.

While ODNI's ability to oversee reciprocity processes at agencies outside of the IC may be improved with the implementation of NBIS, by following best practices for evaluating the reliability of data, ODNI will further improve its access to complete and accurate data. Such access is critical to ODNI's oversight and could improve its awareness of agencies that do not grant clearance reciprocity when they should or are not meeting reciprocity timeliness requirements.

Data OPM Has Collected to Oversee Reciprocity for Suitability, Fitness, and Credentialing Are Not Reliable

OPM officials collect data from CVS to oversee agencies' suitability, fitness, and credentialing determinations. However, the data OPM collects are not reliable because they do not measure reciprocity for these personnel vetting determinations. Instead, the data measure when agencies request a new investigation when there already is an investigation underway or completed that may meet the agency's need—referred to as a duplicate investigation request.[33] As a result, OPM does not have a direct measure of the extent that agencies grant reciprocity, and they are not able to effectively carry out their oversight responsibilities related to reciprocity determinations.

OPM officials stated they are aware that the data they collect do not directly measure reciprocity, but said the data are the only reciprocity-related information available. The officials stated that the data provide an approximate measure of the extent that agencies grant reciprocity for suitability, fitness, and credentialing determinations and therefore have some value to help them fulfill OPM's oversight responsibilities. Specifically, the officials explained that the data measure the inverse of reciprocity. That is, the data measure when an agency could have granted reciprocity but did not. However, OPM officials acknowledged

[33]We also reported on this issue in 2010 in GAO, *Personnel Security Clearances: Progress Has Been Made to Improve Timeliness but Continued Oversight Is Needed to Sustain Momentum*, GAO-11-65 (Washington, D.C.: Nov. 19, 2010).

that the data on duplicate investigations also include data on other events and are thus not reliable.

OPM does not have reliable data because CVS does not allow for the recording of reciprocity determinations for any personnel vetting process, including for suitability, fitness, and credentialing, according to OPM officials. OPM officials told us that they met with the DCSA officials who were developing NBIS and discussed the need to design a capability to address the lack of these data. As a result, these officials stated that DCSA was developing the capability in NBIS that OPM officials said would resolve this gap. Given this planned action, we are not making a recommendation on this issue. When implemented, NBIS may provide additional data that is reliable regarding reciprocity, thereby enabling OPM to better meet its oversight responsibilities.

ODNI and OPM Have Not Fully Addressed Challenges That Agencies and Contractors Face in the Personnel Vetting Reciprocity Processes

ODNI and OPM have taken steps to address challenges in personnel vetting reciprocity that agencies face, but agency respondents to our survey said they continue to experience these challenges. Furthermore, while more than half of contractor respondents to our survey were satisfied with the security clearance reciprocity process, they lacked communication from agencies on the status of reciprocity decisions.

ODNI and OPM Have Taken Steps but Agencies Continue to Face Personnel Vetting Reciprocity Challenges

ODNI and OPM have taken some actions to address personnel vetting reciprocity challenges; however, based on our survey of 31 agencies, we found that these agencies continue to face key challenges in making reciprocity determinations. In particular, agencies reported facing personnel vetting reciprocity challenges related to IT systems. While some suitability and fitness reciprocity challenges may be addressed with the upcoming implementation of NBIS, other reciprocity challenges remain that ODNI and OPM have not yet fully addressed. These challenges are addressed in more detail below. See figure 3 for a summary of the challenges we identified that agencies face.

Figure 3: Summary of Agency Challenges That GAO Identified in the Personnel Vetting Reciprocity Processes

Source: GAO analysis of agency documentation, survey results, and interviews; GAO (design). | GAO-24-105669

Certain IT System Challenges May Be Addressed with Implementation of NBIS

Suitability and fitness: **IT systems cannot record multiple types of vetting determinations.** According to OPM officials, during the initial vetting process, agency officials cannot record determinations for suitability or fitness and security clearances in CVS simultaneously when an employee's current or future position requires both. For example, according to PAC Program Management Office officials, to fill a national security position, an agency must hire an individual who is able to obtain a favorable security clearance determination in addition to a favorable determination for suitability or fitness. However, according to these officials, CVS does not have the capability to record the results of both determinations at the same time.

As a result, agency officials must choose which determination to record. An official from the PAC Program Management Office said agency officials tend to prioritize recording the security clearance determinations in CVS and do not record the suitability or fitness determination because they view the security clearance determination as more important.

Therefore, according to OPM officials, when CVS does not have a record of the suitability or fitness determination, agencies cannot grant suitability or fitness reciprocity if the individual is employed at another agency. OPM officials stated that this IT system capability gap has been a significant challenge for timely determinations of suitability and fitness reciprocity. In these cases, OPM officials said agencies attempting to grant reciprocity must request relevant records from the agency that conducted the investigation.

To address this challenge, OPM officials told us that they submitted a requirement to DCSA to develop the capability to record determinations for security clearances and suitability or fitness in NBIS. In November 2023, a DCSA official told us that DCSA updated NBIS to provide this capability, but that agencies will not be able to use it until NBIS becomes the system of record for agencies.[34] Therefore, we are not making a recommendation on this issue.

Suitability and fitness: IT systems do not include position duties. OPM officials said that CVS and the Defense Information System for Security include information on the type of investigation that was performed and whether the determination was favorable or unfavorable.[35] However, according to OPM officials, CVS and the Defense Information System for Security do not include information about the core duties of an individual's position or the core duties of the new position. They noted that this situation often prevents officials from making suitability or fitness reciprocity determinations.[36] OPM officials told us that without information on the core duties for each position, agencies are not able to grant suitability or fitness reciprocity because the core duties in each position must match.

This situation can be challenging when an individual is hired for a position that differs from the one they held at a prior agency. As part of their hiring processes, agencies check prior background investigation records for any indications that an individual's prior conduct may conflict with the core duties of a new position. For example, if an individual with prior criminal conduct moves from a position with no law enforcement duties to a law enforcement position, the prior criminal conduct could conflict with the core duties of the new law enforcement position, according to OPM

[34]In our August 2023 report, GAO, *Personnel Vetting: DOD Needs a Reliable Schedule and Cost Estimate for the National Background Investigation Services Program* (GAO-23-105670), we raised a matter for congressional consideration suggesting that Congress require DOD to develop a more reliable schedule to track NBIS' development.

[35]According to DOD, the Central Verification System (CVS) is the primary IT system non-DOD agencies use to make reciprocity determinations. It contains information on investigations and determinations for security clearances, eligibility to hold a sensitive position, and suitability, fitness, and credentialing determinations for personnel from most agencies. The Defense Information System for Security is the IT system that DOD officials use to make reciprocity determinations. It contains records for security clearance, suitability, fitness, and credentialing determinations for DOD military personnel, civilians, and contractors.

[36]According to OPM officials, core duties are continuing responsibilities that are of particular importance to the relevant position or the achievement of an agency's mission.

officials. OPM officials told us that in this example, agency officials would need to review the prior background investigation to make a determination for the new position.

OPM officials told us they also provided requirements to DCSA for NBIS to incorporate information about an individual's prior position(s) to facilitate agency officials' ability to make suitability and fitness reciprocity determinations. OPM officials said that DCSA plans to address this requirement as it deploys NBIS and therefore we are not making a recommendation on this issue. While the new NBIS capabilities have not yet been implemented, the future deployment of these capabilities may address the IT limitations agencies face when using legacy IT systems.

Agencies' Plans Will Not Address Additional Personnel Vetting Reciprocity Challenges

Security clearance: agencies sometimes do not trust other agencies' vetting processes. According to ODNI officials, during their assessments of agencies' national security background investigation and adjudication programs, they found that some agencies are not granting reciprocity. These agencies, according to ODNI, believe that other agencies accept levels of risk in their security clearance processes that are too high, resulting in a lack of trust in those agencies' processes.[37] ODNI officials told us that some agencies may reinvestigate or re-adjudicate background investigations before granting reciprocity, which they said is not consistent with the requirements in SEAD 7.[38]

Additionally, of the 31 agencies we surveyed, respondents for 17 stated that they, at times, do not trust other agencies' security clearance

[37]Executive Order 13,467, *as amended*, states that the DNI, as the Security Executive Agent, shall make a continuing review of agencies' national security background investigation and adjudication programs to determine whether they are being implemented according to the executive order. Exec. Order No. 13,467, § 2.5(e), *as amended*. According to a DNI memorandum, to execute this oversight responsibility, the DNI established the Security Executive Agent National Assessments Program. The memorandum states that the program is designed to strengthen programs and provide agencies with the opportunity to address issues or concerns regarding personnel security processes. The memorandum also states that the program will supplement an organization's existing internal oversight mechanisms. DNI Memorandum, *Establishment of the Security Executive Agent National Assessments Program (SNAP)* (Apr. 29, 2014).

[38]See ODNI, SEAD 7, *Reciprocity of Background Investigations and National Security Adjudications* (Nov. 9, 2018).

processes, which can affect their decisions to grant reciprocity.[39] For example, one respondent stated that their agency did not trust other agencies' security clearance processes because some do not require that the results of the polygraph indicate "no significant response" to grant a Top Secret clearance with access to sensitive compartmented information.[40] Another respondent said that other agencies may have inconsistent, or possibly subjective, applications of adjudicative guidelines and investigative standards, which may lead to differences between agencies.

Furthermore, agencies we surveyed reported actions that they took when they did not trust other agencies' security clearance processes. For example, one respondent said their agency may conduct additional work to ensure the investigation is complete and meets federal investigative standards. Another respondent said their agency might require an additional polygraph, an updated interview, or updates and clarification to an existing investigation before granting reciprocity. A third respondent said any information that is in question requires additional review and proper mitigation if necessary.

SEAD 7 requires agencies to accept background investigations completed by an authorized investigative agency that meet all or part of the investigative requirements for a national security background

[39]To calculate data for the 17 of 31 agencies, we combined results for respondents who answered rarely (12), sometimes (4), often (1), and always (0) when asked how often a lack of trust in other agencies' processes and their acceptance of risk in the security clearance process affect decisions to grant reciprocity. For our agency survey, we requested that agencies complete one survey that reflected the organizational perspective.

[40]Some agencies use a polygraph examination as part of their security clearance process. The Director of National Intelligence issued policy governing the use of polygraph examinations in support of personnel security vetting in Security Executive Agent Directive 2, *Use of Polygraph in Support of Personnel Security Determinations for Initial or Continued Eligibility for Access to Classified Information or Eligibility to Hold a Sensitive Position* (Sept. 1, 2020). Furthermore, SEAD 7 states that when a security clearance determination includes a requirement for a polygraph examination, examinations conducted in accordance with Security Executive Agent Directive 2 that are current and consistent with the type and age of examination required by the receiving agency will be reciprocally accepted when the investigation and adjudication meet the requirements for reciprocal acceptance. SEAD 7, § E.3. A polygraph examiner evaluates the physiological data collected during the test and formulates an opinion of the test results. That opinion could be "no significant response," "significant response," or "no opinion." A no significant response opinion would indicate that the examiner did not identify significant physiological responses to the relevant questions. See for example, National Research Council, *The Polygraph and Lie Detection* (Washington, DC: The National Academies Press, 2003).

investigation. There are some exceptions to this requirement, such as when new information of national security adjudicative relevance has been reported or the most recent background investigation is more than 7 years old. SEAD 7 also requires agencies to accept national security eligibility adjudications conducted by authorized adjudicative agencies at the same or higher level, with some exceptions. However, as noted above, some agencies do not trust other agencies' processes and, as a result, do not grant reciprocity though they are required to do so.

To address this challenge, ODNI officials told us they give feedback to agencies that do not trust other agencies' security clearance processes when they identify this issue during assessments of agencies' national security programs. ODNI officials told us they explain the reciprocity requirements and try to dispel the reluctance to grant reciprocity. Despite ODNI's efforts to address this challenge, as noted above, 17 of 31 respondents to our survey said they do not trust other agencies' security clearance processes at times, and ODNI officials pointed out that it was an ongoing challenge. Nevertheless, ODNI has not developed and implemented a plan to address agencies' concerns that led them to mistrust some other agencies' processes. If ODNI develops and implements such a plan, agencies may grant reciprocity more often and avoid duplicative investigative and adjudicative work.

Security clearance: some agencies cannot access a key IT system. Some agencies are not able to review Scattered Castles—one of the three IT systems used to make reciprocity determinations—because it is accessible only from a Sensitive Compartmented Information Facility (SCIF), and these agencies do not have access to a SCIF, according to ODNI officials.[41] For example, two of the 31 agency respondents to our survey reported that their agencies did not have access to Scattered Castles and that this precluded or delayed granting reciprocity for security clearances.

SEAD 7 requires agencies to review relevant IT systems to determine if any prior or current background investigations or national security

[41]A SCIF is an area, room, group of rooms, building, or an installation accredited as meeting ODNI security standards for storing, using, discussing, and handling sensitive compartmented information. See Intelligence Community Standard No. 700-1, *Glossary of Security Terms, Definitions, and Acronyms* (Apr. 4, 2008).

eligibility adjudications exist to make a reciprocity determination.[42] However, ODNI has not facilitated agency access to SCIFs despite maintaining a SCIF repository that may be useful for this purpose. In particular, Intelligence Community Directive 705 requires ODNI to manage an inventory of information on all SCIFs within the IC, including information such as the type of SCIF an agency has and its location, among other information.[43]

To address this challenge, ODNI officials told us they encourage agencies without access to SCIFs to contact agencies that have them to arrange for their use. Notwithstanding ODNI's efforts to address this challenge, ODNI officials acknowledged that SCIF access remains challenging for some agencies. If ODNI facilitates agency access to SCIFs, agencies may be able to grant reciprocity more often and, thus, may avoid duplicative investigative and adjudicative work.

All vetting processes: IT systems have incomplete and inaccurate information. Twenty-eight of the 31 respondents to our survey reported that IT systems, at times, do not have complete information to make reciprocity decisions for all personnel vetting processes.[44] In addition, 26 of the 31 respondents said that IT systems at times contain inaccurate information (see figure 4).[45]

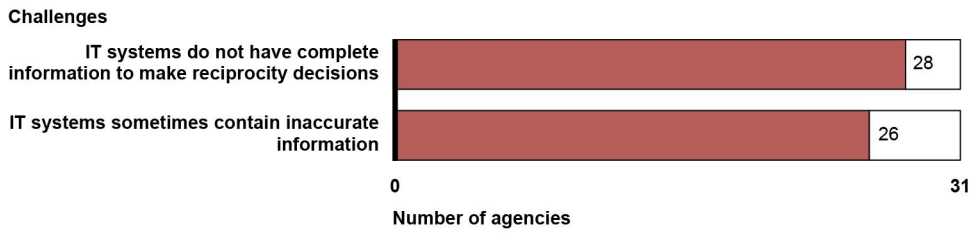
[42]SEAD 7, § E.1.a. The other systems listed in SEAD 7 are DOD's Joint Personnel Adjudication System and OPM's CVS database or successor databases. DOD replaced the Joint Personnel Adjudication System with the Defense Information System for Security on March 31, 2021.

[43]Intelligence Community Directive 705, *Sensitive Compartmented Information Facilities* (May 26, 2010). Specifically, IC elements are responsible for providing ODNI with current information on all SCIFs no later than 30 days after SCIF construction or updated or new information. For purposes of this report, we did not evaluate the completeness or reliability of ODNI's SCIF inventory. In addition, we reported on our assessment of the extent to which ODNI maintains a complete inventory of SCIFs across federal agencies in its government-wide SCIF database in GAO, *Federal Real Property: Improved Data and Access Needed for Employees with Disabilities Using Secure Facilities*, GAO-23-106120SU (Washington, D.C.: Sept. 26, 2023).

[44]In this statistic, we combined results for respondents who answered rarely (9), sometimes (15), often (3), and always (1) when asked how often they encountered incomplete information in CVS, the Defense Information System for Security, or Scattered Castles when making reciprocity decisions.

[45]In this statistic, we combined results for respondents who answered rarely (18), sometimes (6), often (2), and always (0) when asked how often they encountered inaccurate information in CVS, the Defense Information System for Security, or Scattered Castles when making reciprocity decisions.

Figure 4: Number of Executive Branch Agency Respondents That Reported Information Technology (IT) Systems Have Incomplete and Inaccurate Information (n=31)



Source: GAO analysis of survey results. | GAO-24-105669

For example, 11 respondents said that IT systems did not include details needed for reciprocity, such as an individual's final determination or if an individual had a break in federal service. Additionally, another six respondents said IC elements do not enter information about polygraphs into Scattered Castles and that dates for the determination are sometimes missing or outdated. Finally, one other respondent said that information contained in the Defense Information System for Security does not appear in Scattered Castles at times. DCSA officials said that information stored in the Defense Information System for Security and other personnel vetting IT systems is, by design, supposed to appear in Scattered Castles. When it does not, DCSA officials said that agencies must contact a DCSA call center to request a clearance verification.

Similarly, the Office of the Inspector General of the Intelligence Community reported in 2021 that according to IC element security personnel, security clearance IT systems frequently contain incomplete or inaccurate information or are not available when needed.[46] The Inspector General recommended that the Director of the National Counterintelligence and Security Center, in collaboration with the heads of intelligence community elements, ensure that security clearance IT systems contain current, complete, and accurate information required to make reciprocity determinations in accordance with SEAD 7. In July 2023, a senior official from the Office of the Inspector General of the Intelligence Community told us that this recommendation was closed.

ODNI and OPM officials said they have taken several steps to address inaccurate and incomplete information in IT systems. For example, ODNI and OPM issued the *Common Principles for Applying Federal Personnel*

[46]Office of the Inspector General of the Intelligence Community, *Final Report: Evaluation of Intelligence Community Implementation of Security Clearance Reciprocity*, INS-2020-001 (Washington, D.C., Oct. 6, 2021).

Vetting Adjudicative Standards. The standards state that adjudicators must record personnel vetting trust determinations in the individual's federal personnel vetting record. They also state that accurately recording personnel vetting actions and determinations enhances mobility, among other things.[47]

Furthermore, as part of their agency's government-wide oversight responsibility, OPM officials said they established an assessment program to validate agencies' compliance with requirements regarding suitability, fitness, and credentialing programs. OPM officials told us their oversight teams annually carry out a detailed assessment of the vetting programs of about 15 organizations in agencies. During these assessments, OPM officials said their oversight teams check to determine if agencies adhere to the requirements to report the results of background investigations in CVS. OPM teams make recommendations to agencies not adhering to these requirements.

Despite ODNI's and OPM's actions, 22 of 31 respondents to our survey reported that incomplete and inaccurate information in IT systems was the most significant challenge they faced when attempting to grant reciprocity. This issue exists because ODNI and OPM have not developed and implemented a plan to ensure that current and future IT systems used for personnel vetting contain complete and accurate information required to make reciprocity determinations. *Standards for Internal Control in the Federal Government* state that management should use quality information to achieve the entity's objectives. Quality information is complete, accurate as well as appropriate, current, accessible, and provided on a timely basis.[48] If ODNI and OPM develop and implement such a plan, agencies may avoid conducting duplicative investigative and adjudicative work.

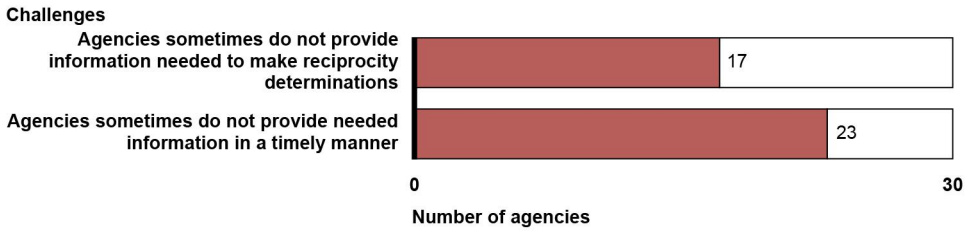
All vetting processes: agencies sometimes do not communicate effectively with each other. Agencies at times do not communicate effectively with each other when requesting additional information from an individual's prior agency or investigative service provider to enable a reciprocity determination. For example, 17 of 30 executive branch agency survey respondents reported that other agencies, at times, do not provide

[47]DNI and Director of OPM, *Common Principles for Applying Federal Personnel Vetting Adjudicative Standards* (July 19, 2022).

[48]GAO, *Standards for Internal Control in the Federal Government,* GAO-14-704G (Washington, D.C.: September 2014).

the information needed to make reciprocity determinations.[49] In addition, 23 of the 30 respondents said that other agencies sometimes do not provide needed information promptly (see figure 5).[50]

Figure 5: Number of Executive Branch Agency Respondents Reporting That Agencies Do Not Communicate Effectively with Other Agencies (n=30)



Source: GAO analysis of survey results. | GAO-24-105669

Standards for Internal Control in the Federal Government state that management should communicate with—and obtain quality information from—external parties, including government entities, using established reporting lines.[51] However, we found that agencies do not communicate effectively with each other for two reasons. First, because ODNI has not issued clarifying guidance, such as by updating SEAD 7, to address whether communicating with prior agencies is permitted in the process for security clearance reciprocity and, if so, under what circumstances it is allowable. The second reason is because OPM has not developed and implemented supplemental policies to ensure that agencies consistently share reciprocity-related information for suitability, fitness, and credentialing.

Regarding ODNI, its officials provided conflicting information at different points during our review on the role of communication in the reciprocity process. For example, in January 2023, ODNI officials told us that

[49]Thirty of the 31 agencies we surveyed responded to our question about the extent that other agencies provided information to facilitate reciprocity. To calculate data about the 17 of 30 agencies, we combined results for respondents who answered rarely (10), sometimes (5), often (1), and always (1) when we asked how often agencies declined to share information needed to make a reciprocity decision about an individual.

[50]Thirty of the 31 respondents from agencies responded to our question about the extent that other agencies provided information in a timely manner to facilitate reciprocity. In addition, to calculate the 23 of 30 statistic, we combined results for respondents who answered rarely (8), sometimes (12), often (2), and always (1) when we asked how often agencies did not respond to requests in a timely manner for information about an individual.

[51]GAO-14-704G.

agencies sometimes do not communicate effectively in the reciprocity process and that ODNI was taking steps to address this issue. One such step was that ODNI had described the collaboration needed among agencies for reciprocity to occur effectively in various forums and working groups. However, in July 2023, ODNI officials said that information sharing is not part of the reciprocity process. For example, a senior ODNI official told us that an agency calling officials at a prior agency to ask for clarification about an individual's background investigation or determination would not be part of the reciprocity process. SEAD 7 does not clarify whether, how, and when communication with prior agencies is or could be permitted as part of the reciprocity process.[52]

However, if communicating with prior agencies is not permitted, responses to our survey indicate that many agencies are not aware of this. For example, 30 of the 31 respondents to our survey indicated that they communicated with other agencies at times as a matter of course when attempting to grant reciprocity. In addition, security officials responsible for reciprocity processes at some of the agencies we interviewed told us they communicated with prior agencies during the process. For example, officials from one agency told us that CVS sometimes includes an alert in an individual's file that requires agencies to contact the former agency prior to granting reciprocity.

Regarding OPM's response to this challenge, an OPM official acknowledged that agencies, at times, do not effectively communicate information needed for reciprocity. This official said that a contributing factor to this problem is that IT systems sometimes do not have accurate contact information. This official said DCSA has plans to address this issue in NBIS.

If ODNI issues clarifying guidance, such as by updating SEAD 7, to address the role of communication with prior agencies in the reciprocity process, and if OPM develops and implements policies to ensure that agencies share information to facilitate reciprocity, agencies may avoid conducting duplicative investigative and adjudicative work and may grant reciprocity in a timelier manner.

[52]See SEAD 7.

More Than Half of Contractors Were Satisfied with the Security Clearance Reciprocity Process but They Cited a Lack of Communication from Agencies

More than half of the private organizations that perform contracting work for the federal government who responded to our survey were extremely or somewhat satisfied with this process. Specifically, 20 of 109 contractor respondents reported that they were extremely satisfied, and 46 reported that they were somewhat satisfied. However, some respondents to our survey expressed concerns with the lack of communication regarding the status of reciprocity decisions. Specifically, 40 of 48 contractor respondents reported that agencies never or rarely provide information about the status of a reciprocity request when there were delays.[53]

Furthermore, contractor respondents we surveyed said that receiving status updates could benefit the government. Specifically, 54 of the 109 respondents reported that receiving status updates would help contractors in project planning, hiring, retaining employees, and providing updates to prospective employees and government clients, among other benefits. Respondents also reported that receiving status updates would enable contractors to provide government clients with better information about the status of the contracts.

Standards for Internal Control in the Federal Government state that management should externally communicate the necessary quality information through reporting lines so that external parties, which include contractors, can help them achieve their objectives and address related risks.[54]

[53]Of the 293 contractors who responded to our survey, 109 reported they had recent experience related to security clearance reciprocity. We included responses only from the 109 who had recent experience with reciprocity to ensure that their responses were informed by current trends in the reciprocity processes. We defined recent experience as occurring in the most recent 3 fiscal years (i.e., 2020 through 2022). In addition, only 48 contractors responded to the question we asked about the extent that agencies provide information about the status of a reciprocity request. SEAD 7 requires agencies to make reciprocity determinations for security clearance background investigations and determinations within 5 business days from the date that they receive the request. In some cases, agencies must obtain investigative records from another agency to make reciprocity decisions, which adds time to the process. In such cases, SEAD 7 requires the agency with the investigative records to provide them to the requesting agency within 10 business days of the request. SEAD 7, § G.

[54]GAO-14-704G.

ODNI officials told us they were aware that contractors would like to receive these status updates, but they said it was not feasible for agencies to notify contractors because of the large volume of requests for reciprocity of security clearances. However, officials from two agencies told us their agencies already provide status updates to contractors and an official from a third agency said sending regular updates could be feasible if the process was automated. Further, a PAC Program Management Office official stated that agencies cannot share the underlying information that is causing a delay and it is difficult to gauge how long it will take them to address the cause of a delay.

Contractors are not always informed about the status of reciprocity determinations for security clearances when there are delays because ODNI has not developed and implemented a plan for such updates. If ODNI develops and implements a plan that accounts for contractor and agency concerns—with consideration of resource and privacy issues—to communicate status updates to contractors, they may have better information to plan projects and hire personnel, which could have positive effects on fulfilling government contracts.

Conclusions

Personnel vetting is critical to protecting the nation's interests by providing a means to establish and maintain trust in the federal government's workforce. In addition, a process that efficiently enables agencies to grant reciprocity for prior vetting determinations is key to enabling personnel mobility, which can help agencies access personnel with the skills needed to accomplish their missions.

Yet, ODNI collected data that were not sufficiently reliable to determine the extent to which agencies granted security clearance reciprocity. By following best practices for evaluating the reliability of the data agencies report, ODNI will have access to additional data that is complete and accurate, which will enable ODNI to conduct more effective oversight. Such access is critical to ODNI's oversight and could improve its awareness of agencies that do not grant clearance reciprocity when they should or are not meeting reciprocity timeliness requirements.

Additionally, it will be important that DCSA follow through on plans to implement capabilities in NBIS to address limitations in CVS that hinder suitability and fitness reciprocity. In particular, it will be important for DCSA to implement capabilities to record reciprocity determinations,

adjudications for suitability or fitness and security clearances for individuals who require both, and information about an individual's prior position.

Further, agencies continue to face key challenges in making reciprocity determinations for all vetting processes. By developing and implementing a plan that addresses agencies' concerns, ODNI may be able to mitigate the lack of trust some agencies have in other agencies' security clearance processes. In addition, by facilitating access to SCIFs for agencies that do not have one, ODNI may help agencies access secure facilities to review records in Scattered Castles. In addition, if ODNI and OPM develop a plan to ensure that current and future IT systems contain complete and accurate information, these agencies will have better information to make reciprocity decisions.

Moreover, if ODNI issues clarifying guidance, such as by updating SEAD 7, to address whether communicating with prior agencies is permitted in the reciprocity process and under what circumstances, it will help ensure that agencies are taking actions consistent with requirements. Also, if OPM develops and implements policies to ensure that agencies share information about suitability, fitness, and credentialing, agencies will have additional information needed for reciprocity. Finally, if ODNI develops a plan that accounts for contractor and agency concerns—with consideration of resource and privacy issues—to ensure that contractors are regularly informed about the status of reciprocity for security clearances, and implements that plan, contractors will have better information to plan projects and hire personnel.

By taking these actions, ODNI and OPM will enable agencies to grant reciprocity more often and more quickly. Improved reciprocity will enable agencies to access personnel with needed skills more quickly and help those agencies achieve their missions.

Recommendations for Executive Action

We are making eight recommendations: six to the Director of National Intelligence in its role as the Security Executive Agent, and two to the Director of the Office of Personnel Management in its role as the Suitability and Credentialing Executive Agent:

The Director of National Intelligence should follow best practices for evaluating the reliability of the data that agencies submit related to

security clearance reciprocity. Such best practices include interviewing knowledgeable officials about their data systems, reviewing data system documentation to determine if data entry controls are sufficient, and tracing a sample of data to or from source documents to assess the accuracy and completeness of the data. (Recommendation 1)

The Director of National Intelligence should develop and implement a plan that addresses agencies' concerns that led them to mistrust some other agencies' security clearance processes. (Recommendation 2)

The Director of National Intelligence should facilitate access to secure facilities and systems for agencies to ensure they can make reciprocity determinations. (Recommendation 3)

The Director of National Intelligence, in coordination with the Director of the Defense Counterintelligence and Security Agency, should develop and implement a plan to ensure that current and future IT systems used for personnel vetting contain complete and accurate information required to make security clearance reciprocity determinations. (Recommendation 4)

The Director of the Office of Personnel Management, in coordination with the Director of the Defense Counterintelligence and Security Agency, should develop and implement a plan to ensure that current and future IT systems used for personnel vetting contain complete and accurate information required to make suitability, fitness, and credentialing reciprocity determinations. (Recommendation 5)

The Director of National Intelligence should issue clarifying guidance, such as by updating Security Executive Agent Directive 7, to address whether communicating with prior agencies is permitted in the security clearance reciprocity process and, if so, under what circumstances. (Recommendation 6)

The Director of the Office of Personnel Management should develop and implement supplemental policies to ensure that federal agencies consistently share information with other agencies attempting to grant suitability, fitness, and credentialing reciprocity. (Recommendation 7)

The Director of National Intelligence should develop and implement a plan that accounts for contractor and agency concerns—with consideration of resource and privacy issues—to ensure that contractors

are informed about the status of reciprocity determinations when there are delays. (Recommendation 8)

Agency Comments

We provided a draft of this report to OPM, ODNI, DOD, and the Office of Management and Budget for review and comment. OPM provided written comments that we reprinted in their entirety in appendix II. ODNI did not provide comments stating whether it concurred with the recommendations directed to it, but provided technical comments which we incorporated as appropriate. DOD and the Office of Management and Budget also provided technical comments, which we incorporated in the report as appropriate.

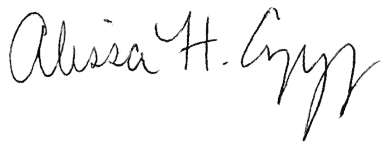
In its comments, OPM concurred with our recommendation that it develop and implement a plan to ensure that IT systems contain complete and accurate information to make suitability, fitness, and credentialing reciprocity determinations. While OPM did not specifically state how it would address this recommendation, it agreed that enhancements to the reciprocity system are needed to improve the mobility of individuals. OPM also stated that it will continue to work with DCSA regarding the requirements for the National Background Investigation Services IT system.

OPM also concurred with our recommendation that it should develop and implement supplemental policies to ensure that federal agencies consistently share information with other agencies attempting to grant suitability, fitness, and credentialing reciprocity. In particular, OPM stated that it agrees with the importance of accurate and timely reporting and sharing of information within and across agencies. OPM also stated that it will develop and implement policies that promote timely information sharing among agencies by building on Trusted Workforce 2.0 policies that have emphasized information sharing. For example, OPM stated that, in the Federal Personnel Vetting Core Doctrine, ODNI and OPM described that for policy priorities to be successful, they must promote and enable multi-directional information sharing. Further, OPM stated that the Federal Personnel Vetting Guidelines address the federal personnel vetting record and information sharing as critical personnel vetting elements.

We are sending copies of this report to the appropriate congressional committees, the Director of National Intelligence, the Director of OPM, the

Secretary of Defense, and the Director of the Office of Management and Budget. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-3058 or CzyzA@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix III.



Alissa H. Czyz
Director, Defense Capabilities and Management

Appendix I: Objectives, Scope, and Methodology

The objectives of this report were to evaluate the extent to which the Office of the Director of National Intelligence (ODNI) and the Office of Personnel Management (OPM) (1) collected complete and accurate information about reciprocity in the personnel vetting processes and (2) addressed challenges that agencies and contractors face in the personnel vetting reciprocity processes.

For our first objective, we reviewed Executive Order 13,467, which includes requirements related to reciprocity for all three personnel vetting processes.[1] We also reviewed policies for each of the vetting processes including:

- **Eligibility for access to classified information or to hold a sensitive position (security clearance process)**.[2] The Director of National Intelligence's (DNI) November 2018 Security Executive Agent Directive (SEAD) 7, Reciprocity of Background Investigations and National Security Adjudications.[3]
- **Suitability and fitness**. Part 731 of title 5, Code of Federal Regulations, Suitability.[4]
- **Credentialing**. The Director of OPM's December 2020 memorandum, Credentialing Standards Procedures for Issuing Personal Identity Verification Cards under HSPD-12 and New Requirement for

[1]See Exec. Order No. 13,467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*, § 2.2, *as amended through* Exec. Order No. 13,869, *Transferring Responsibility for Background Investigations to the Department of Defense,* 84 Fed. Reg. 18,125 (Apr. 24, 2019).

[2]For the purposes of this report, we use the term security clearance process to refer to the process to determine eligibility for access to classified information or eligibility to hold a sensitive position.

[3]Office of the Director of National Intelligence, Security Executive Agent Directive 7 (SEAD 7), *Reciprocity of Background Investigations and National Security Adjudications* (Nov. 9, 2018) establishes requirements for reciprocal acceptance of background investigations and national security adjudications for initial or continued eligibility for access to classified information or eligibility to hold a sensitive position.

[4]5 C.F.R. part 731 (2023).

Suspension or Revocation of Eligibility for Personal Identity Verification Credentials.[5]

Analysis of ODNI Data on Reciprocity for Security Clearances

To assess ODNI's efforts to collect information from agencies on reciprocity for security clearance determinations, we reviewed a memorandum the Director of the National Counterintelligence and Security Center, at the direction of the Director of National Intelligence, issued in 2019. The memorandum required agencies to report data quarterly on security clearance topics to ODNI.[6] We also reviewed information that ODNI provided about its Security Executive Agent National Assessments Program. This program is designed to strengthen agencies' security clearance programs and provide agencies the opportunity to address issues or concerns regarding personnel security processes.[7] Further, we reviewed reports ODNI issued on the findings of these assessments for several agencies, including the U.S. Agency for International Development, the Defense Information Systems Agency, and the Defense Contract Management Agency.

Moreover, we reviewed planning documents from the Defense Counterintelligence and Security Agency on the National Background Investigation Services Information Technology (IT) system. In addition, we reviewed audit reports prepared by the Intelligence Community Inspector General's office on the processes Intelligence Community (IC)

[5]Director of OPM Memorandum, *Credentialing Standards Procedures for Issuing Personal Identity Verification Cards under HSPD-12 and New Requirement for Suspension or Revocation of Eligibility for Personal Identity Verification Credentials* (Dec. 15, 2020) was issued by OPM to promote defined goals in agency eligibility determinations to issue Homeland Security Presidential Directive 12 personnel identification credentials for access to federally controlled facilities and information systems.

[6]DNI Memorandum, *Metrics Reporting Requirements for National Security Vetting in Fiscal Year 2018 and Beyond* (Nov. 19, 2018); Director of the National Counterintelligence and Security Center Memorandum, *Metrics Reporting Requirements for National Security Vetting in Fiscal Year 2018 and Beyond* (Jan. 18, 2019).

[7]DNI Memorandum, *Establishment of the Security Executive Agent National Assessments Program (SNAP)* (Apr. 29, 2014),

elements use for security clearance reciprocity.[8] Further, we reviewed our prior reports with relevant findings on security clearance reciprocity.[9]

In addition, we obtained data from ODNI on the frequency that agencies granted reciprocity for security clearances in fiscal years 2019 through 2021.[10] We chose these years because at the time we started our review, these were the 3 most recent fiscal years. We assessed the reliability of these data by (1) reviewing documentation related to the data, (2) reviewing the data for missing values, (3) interviewing knowledgeable ODNI officials about their collection and analysis methods for these data, and (4) interviewing knowledgeable officials from a nongeneralizable selection of five executive branch agencies about their data collection, storage, and reporting to ODNI.

To select these agencies, we considered multiple factors to obtain a diverse set of perspectives. In particular, we selected five agencies from various sectors of the executive branch including defense, intelligence, and nondefense and nonintelligence. We also considered the number of employees in the department or agency and whether they had the authority to conduct background investigations, according to ODNI. The five agencies we selected are:

- U.S. Agency for International Development
- Drug Enforcement Administration
- Defense Counterintelligence and Security Agency
- Defense Intelligence Agency
- Department of Veterans Affairs

[8]Office of the Intelligence Community Inspector General, *Final Report: Evaluation of Intelligence Community Implementation of Security Clearance Reciprocity*, INS-2020-001 (Washington, D.C., Oct. 6, 2021) and Office of the Intelligence Community Inspector General, *Audit Report of Intelligence Community Security Clearance Reciprocity*, IC IG-AUD-2012-005 (Washington, D.C.: December 2012).

[9]In particular, we reviewed relevant findings in GAO, *Personnel Security Clearances: Progress Has Been Made to Improve Timeliness but Continued Oversight Is Needed to Sustain Momentum*, GAO-11-65 (Washington, D.C.: Nov. 19, 2010) and GAO, *Personnel Security Clearances: Funding Estimates and Government-Wide Metrics Are Needed to Implement Long-Standing Reform Efforts*, GAO-15-179SU (Washington, D.C.: Apr. 23, 2015).

[10]Throughout this report, we use the term *agencies* to refer to both executive branch departments and agencies where appropriate.

In addition, we compared ODNI actions related to data on reciprocity for security clearances to criteria in the *Standards for Internal Control in the Federal Government* related to management's use of quality information to achieve its objectives.[11] We found that ODNI's data were not sufficiently reliable to determine the extent that agencies granted reciprocity for security clearances, or the time agencies took to complete the process.

Analysis of OPM Data on Reciprocity for Suitability, Fitness, and Credentialing

We assessed the reliability of data that OPM uses to determine the extent to which agencies grant reciprocity for suitability, fitness, and credentialing determinations. We reviewed documentation about the data OPM analyzes from the Central Verification System (CVS). We also reviewed OPM oversight reports that included findings on agencies' processes for reciprocity of suitability, fitness, and credentialing determinations. Further, we reviewed our 2010 report that included a finding on the data OPM uses to assess suitability, fitness, and credentialing reciprocity.[12] We also interviewed knowledgeable officials from the five selected agencies we identified above. We found the data OPM used were not sufficiently reliable to determine the extent that agencies granted reciprocity for suitability, fitness, and credentialing. Further, we compared OPM actions related to data on reciprocity for suitability, fitness, and credentialing determinations to best practices we established in a guide on assessing the reliability of data.[13]

Analysis of Reciprocity-Related Challenges That Agencies and Contractors Face

For our second objective, we obtained information about challenges agencies face when attempting to grant reciprocity for personnel vetting determinations by interviewing officials from ODNI, OPM, the Department of Defense (DOD), and the five selected agencies we used for our first

[11]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: September 2014).

[12]GAO, *Personnel Security Clearances: Progress Has Been Made to Improve Timeliness but Continued Oversight Is Needed to Sustain Momentum*, GAO-11-65 (Washington, D.C.: Nov. 19, 2010).

[13]GAO, *Assessing Data Reliability*, GAO-20-283G (Washington, D.C.: Dec. 16, 2019).

objective. We then selected and surveyed 31 agencies to identify and better understand challenges within the reciprocity processes. Our selection process is explained below.

We used a similar approach to identify the reciprocity-related challenges that contractors faced. In particular, we interviewed officials with experience requesting that agencies grant reciprocity for personnel vetting determinations for personnel in their companies. We also reviewed reciprocity-related reports from the Intelligence and National Security Alliance. [14] In addition, we interviewed officials from ODNI, OPM, DOD, and the Performance Accountability Council Program Management Office. To obtain a broader range of perspectives on these issues, we surveyed a nongeneralizable sample of 600 small and large contractors. Of the 600 we contacted, 293 responded (described in more detail below).

Agency Survey Methods

Agency Sample Selection

We selected a nongeneralizable sample of 31 agencies from a universe of 83 agencies in four categories: cabinet-level departments, large- and medium-sized independent agencies, and IC elements. We included each of the 15 cabinet-level departments because they represent a broad cross-section of the executive branch. From the 17 IC elements, excluding ODNI, we selected the six IC elements whose personnel comprise 80 percent of the IC workforce. Further, unlike most agencies, these IC elements have the delegated authority to conduct their own background investigations according to ODNI, which helped to diversify the perspectives in our sample.

In addition, we used OPM agency-size definitions to select five independent agencies from a group of 22 large-sized agencies and five independent agencies from a group of 30 medium-sized agencies. To

[14]Intelligence and National Security Alliance, *Security Clearance Reciprocity: Obstacles and Opportunities* (June 2019); Intelligence and National Security Alliance, *Security Clearance Reciprocity: National Standards and Best Practices Would Expedite Clearance Transfers* (July 2017). According to its website, this organization is a nonprofit, nonpartisan membership association that works on intelligence and national security issues.

select these 10 agencies, we selected the agencies with the most personnel in each of these two size categories.

Although our sample is nongeneralizable, the information obtained from these agencies offered useful insights and perspectives on reciprocity challenges and how to address them.

Agency Survey Development

After identifying our sample, we developed our survey with the assistance of knowledgeable and independent GAO survey experts. We then pretested the survey separately with officials at four agencies. We selected officials to participate in our pretests who had experience making reciprocity decisions to ensure that we (1) asked questions clearly, (2) used terminology correctly, (3) did not place an undue burden on agency officials, (4) asked for information that officials could feasibly obtain, and (5) asked comprehensive and unbiased questions. In response to the feedback that we received in our pretests, we revised the content and format of the survey.

Agency Survey Administration

Next, we requested that agencies in our sample complete one survey on behalf of their department or agency to represent the organizational view. To help achieve this goal, we asked them to identify an official to coordinate and collect input from other relevant officials internally when responding to the survey. We launched the survey on October 31, 2022, by email. The email included a hyperlink to the web-based survey, which we hosted on a secure server. We sent follow-up emails to non-respondents at different points in time and ultimately achieved a 100-percent response rate.

Contractor Survey Methods

Contractor Sample Selection

To survey contractors about the reciprocity-related challenges they faced, we selected a nongeneralizable sample of 600 contractors from the National Industrial Security System (NISS). The Defense Counterintelligence and Security Agency maintains NISS as the system of record for information on contractors that are a part of the National Industrial Security Program. NISS includes data on contractor facilities

that are cleared to access classified information. We chose this database to select our sample because it contained information on a significant number of contractors and the database included contact information for personnel who have experience requesting reciprocity for personnel vetting determinations. To select our sample from NISS, we included only active contractors with a Secret or Top Secret clearance. Further, although NISS contained records for multiple facilities for some contractors, we selected only one facility per contractor to diversify the perspectives in our sample.

We also used data from the Federal Procurement Data System (FPDS) to identify certain contractors in the NISS data. FPDS is the federal government's database that contains information on contracts that agencies have awarded. In particular, we added some data from FPDS to our NISS data where both databases had information about the same contractor. We then used the FPDS data to identify and exclude contractors from the NISS data that supported only one agency in fiscal year 2021 because we assumed that those contractors would have had fewer opportunities to request reciprocity for their personnel.

We also used FPDS and NISS data to select a mix of small and large contractors. We defined contractors in NISS as small business contractors if FPDS reported 95 percent or more of their obligations as a small business based on the contracting officer's business size selection for fiscal year 2021. Using this approach, we identified 3,037 small business contractors in NISS and we randomly selected 200. For large business contractors, we included 14 contractors that NISS identified as the largest and most complex. NISS also contained 1,477 contractors that FPDS data identified as other than small, which we defined as a large business contractor. We randomly selected 186 contractors from this category. Coupled with the 14 contractors that NISS identified as the largest and most complex, this constituted 200 large business contractors. We also randomly selected 200 contractors from the 3,310 contractors in NISS for which FPDS did not include any information to enable us to categorize it as a small or large business. Although we randomly selected participants within each of these three categories for this survey, these results are not generalizable to all contractors.

While our sample is nongeneralizable, the information we obtained from these contractors offered useful insights and perspectives on reciprocity challenges and how to address them.

Contractor Survey Development

As in our survey of departments and agencies, we developed our survey of contractors with the assistance of knowledgeable and independent GAO survey experts. We then pretested the survey in four separate meetings each with one facility security official from a contractor with experience requesting reciprocity. In response to the feedback we received in our pretests, we revised the content and format of the survey.

Contractor Survey Administration

We sent our survey to one security official employed by each contractor and asked them to confirm that they had experience requesting agencies to grant reciprocity for contractor employees from 2019 through 2021. We launched the survey on December 8, 2022, by email. The email included a hyperlink to the web-based survey, which we also hosted on a secure server. We sent four follow-up emails to those who had not responded. We made the survey available until January 13, 2023. Ultimately, we received completed surveys from 293 of 600 contractors resulting in a 49-percent response rate.

Analysis of Findings

We analyzed the responses to the surveys, including the closed-ended and open-ended questions. For the closed-ended questions, we analyzed the responses to identify themes and trends in the quantitative results. For the open-ended responses, we performed content analysis on the open-ended responses to questions to identify themes across the respondents. To complete this work, two GAO analysts identified and agreed on themes regarding challenges in the responses to each open-ended question. The analysts then categorized each response into one or more themes and reached consensus on the final categorization.

Analysis of Executive Agent Actions to Address Challenges and Comparison of Agency Actions to Requirements and Principles

Finally, we reviewed documentation and interviewed ODNI and OPM officials about how they were addressing the challenges that agencies and contractors identified in the surveys. Also, we compared agency actions to grant reciprocity and review IT systems to requirements that the Director of National Intelligence established for security clearance

reciprocity in SEAD 7. We also compared agency actions to principles established in *Standards for Internal Control in the Federal Government*. Specifically, we compared those actions to the following principles:

- include complete and accurate information in IT systems used for reciprocity,
- communicate with other agencies about reciprocity, and
- communicate with contractors.

We conducted this performance audit from January 2022 to January 2024 in accordance with generally accepted government auditing standards.[15] Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[15]Our time frames for completing our review were affected, in part, by delays in obtaining needed information.

Appendix II: Comments from the Office of Personnel Management

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Suitability Executive Agent Programs

Alissa H. Czyz
Director
Defense Capabilities and Management
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Czyz:

Thank you for providing us the opportunity to respond to the Government Accountability Office (GAO) draft report, *Federal Workforce: Actions Needed to Improve the Transfer of Personnel Security Clearances and Other Vetting Determinations*, GAO-24-105669SU.

Responses to your recommendations are provided below. In addition, a technical comment is attached.

Recommendation #5: The Director of the Office of Personnel Management, in coordination with the Director of DCSA, should develop and implement a plan to ensure that current and future IT systems used for personnel vetting contain complete and accurate information required to make suitability, fitness, and credentialing reciprocity determinations.

Management Response: We concur. OPM agrees that enhancements to the government-wide reciprocity system are necessary for improving mobility of individuals as they transfer from one agency to another and for allowing for effective oversight of agency compliance with reciprocity requirements. OPM will continue to work with DCSA regarding the requirements for the National Background Investigation Services (NBIS) to validate that they capture more than one type of adjudicative determination so that agencies will not have to choose which of their adjudicative decisions to report. Having all adjudicative determinations visible in the system will avoid delays due to agencies needing to request files from the Investigative Service Provider or reach out to other agency adjudicative offices to request information. In addition, OPM will continue to address with DCSA, the need for NBIS to capture with more specificity, the nature of conduct in an individual's background. This will allow agencies to make determinations to discern, for example, whether there may be a core duty conflict without having to request and review the prior investigation.

Additionally, OPM has provided input to DCSA on how to capture the basis for when an agency does not apply reciprocity. Through continual testing of the NBIS systems, OPM will work with the NBIS development team on refining these fields, as necessary. Developing capabilities to allow for data tracking and trend identification would assist in oversight and/or determinations of whether agencies are properly applying reciprocity policies.

The ongoing coordination between OPM and DCSA is tracked and monitored by a DOD managed Personnel Vetting Requirements Council (PVRC). The PVRC is the principal entity responsible for gathering personnel vetting capabilities from DoD, other Federal partners, and industry stakeholders. The PVRC collects and validates operational and system capabilities to assist DCSA in developing, operating, and continuously improving enterprise personnel vetting systems. The PVRC was designed to improve stakeholder engagement, provide a single entry-point for desired personnel vetting capabilities, and establish standard processes to prioritize these capabilities. OPM as an advisory member, will continue to leverage the PVRC in support of implementing these new requirements.

Recommendation #7: The Director of the Office of Personnel Management should develop and implement supplemental policies to ensure that federal agencies consistently share information with other agencies attempting to grant suitability, fitness, and credentialing reciprocity.

Management Response: We concur. OPM agrees with the importance of accurate and timely reporting and sharing of information within and across agencies and will develop and implement policies that promote timely information sharing among agencies, building upon these aspects that have been points of emphasis in Trusted Workforce 2.0 policies and issuances. In the Federal Personnel Vetting Core Doctrine, the OPM and Office of the Director of National Intelligence (ODNI) Directors, in their capacity as the Suitability and Credentialing and Security Executive Agents, described that for policy priorities to be successful, they must promote and enable multi-directional information-sharing to the greatest extent practical to identify risk in a timely manner, reduce waste, improve quality, increase effectiveness, and maximize efficiency. Additionally, properly managing and safeguarding information is essential to good government, maintaining the trust of the public and the workforce, and the quality and effectiveness of operations. In the Federal Personnel Vetting Guidelines, the Federal personnel vetting record and information sharing are addressed as critical personnel vetting elements. Departments and agencies must record personnel vetting determinations, to include investigative items and adjudicative information, in the government-wide repositories and internal systems, for increased mobility and transparency. Sharing information across and within departments and agencies eliminates unnecessary duplication and reduces waste. Information sharing also improves transparency of the process, ensures quality, and maximizes efficiency. In the Common Principles in Applying Federal Personnel Vetting Adjudicative Standards, adjudicators are reminded of the responsibility to record personnel vetting actions and determinations because accurately reporting this information promotes transparency, enhances mobility, and facilitates information sharing. This includes reporting reciprocal acceptance of determinations.

OPM is developing jointly with ODNI additional policy guidance for personnel vetting management that will be addressed to personnel vetting program practitioners at federal agencies. This policy will establish requirements for Executive Branch personnel vetting programs to apply sound risk management practices to assess the trustworthiness of individuals who work for or on behalf of the Federal government. With this policy, the Executive Agents can provide specific requirements for departments and agencies with respect to information sharing and can reemphasize the requirement for timely and accurate reporting.

I appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact Christine Bilunka at Christine.Bilunka@opm.gov.

Sincerely,

LISA LOSS Digitally signed by LISA LOSS Date: 2023.12.04 18:42:27 -05'00'

Lisa M. Loss
Suitability Director
U.S. Office of Personnel Management
Suitability Executive Agent Programs

Attachment

Accessible Text for Appendix II: Comments from the Office of Personnel Management

Alissa H. Czyz
Director
Defense Capabilities and Management
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Czyz:

Thank you for providing us the opportunity to respond to the Government Accountability Office (GAO) draft report, Federal Workforce: Actions Needed to Improve the Transfer of Personnel Security Clearances and Other Vetting Determinations, GAO-24-105669SU.

Responses to your recommendations are provided below. In addition, a technical comment is attached.

Recommendation #5: The Director of the Office of Personnel Management, in coordination with the Director of DCSA, should develop and implement a plan to ensure that current and future IT systems used for personnel vetting contain complete and accurate information required to make suitability, fitness, and credentialing reciprocity determinations.

Management Response: We concur. OPM agrees that enhancements to the government-wide reciprocity system are necessary for improving mobility of individuals as they transfer from one agency to another and for allowing for effective oversight of agency compliance with reciprocity requirements. OPM will continue to work with DCSA regarding the requirements for the National Background Investigation Services (NBIS) to validate that they capture more than one type of adjudicative determination so that agencies will not have to choose which of their adjudicative decisions to report.

Having all adjudicative determinations visible in the system will avoid delays due to agencies needing to request files from the Investigative Service Provider or reach out to other agency adjudicative offices to request information. In addition, OPM will continue to address with DCSA, the need for NBIS to capture with more specificity, the nature of conduct in an individual’s background. This will allow agencies to make determinations to discern, for example, whether there may be a core duty conflict without having to request and review the prior investigation.

Additionally, OPM has provided input to DCSA on how to capture the basis for when an agency does not apply reciprocity. Through continual testing of the NBIS systems,

OPM will work with the NBIS development team on refining these fields, as necessary. Developing capabilities to allow for data tracking and trend identification would assist in oversight and/or determinations of whether agencies are properly applying reciprocity policies.

The ongoing coordination between OPM and DCSA is tracked and monitored by a DOD managed Personnel Vetting Requirements Council (PVRC). The PVRC is the principal entity responsible for gathering personnel vetting capabilities from DoD, other Federal partners, and industry stakeholders. The PVRC collects and validates operational and system capabilities to assist DCSA in developing, operating, and continuously improving enterprise personnel vetting systems. The PVRC was designed to improve stakeholder engagement, provide a single entry- point for desired personnel vetting capabilities, and establish standard processes to prioritize these capabilities. OPM as an advisory member, will continue to leverage the PVRC in support of implementing these new requirements.

Recommendation #7: The Director of the Office of Personnel Management should develop and implement supplemental policies to ensure that federal agencies consistently share information with other agencies attempting to grant suitability, fitness, and credentialing reciprocity.

Management Response: We concur. OPM agrees with the importance of accurate and timely reporting and sharing of information within and across agencies and will develop and implement policies that promote timely information sharing among agencies, building upon these aspects that have been points of emphasis in Trusted Workforce 2.0 policies and issuances. In the Federal Personnel Vetting Core Doctrine, the OPM and Office of the Director of National Intelligence (ODNI) Directors, in their capacity as the Suitability and Credentialing and Security Executive Agents, described that for policy priorities to be successful, they must promote and enable multi-directional information- sharing to the greatest extent practical to identify risk in a timely manner, reduce waste, improve quality, increase effectiveness, and maximize efficiency. Additionally, properly managing and safeguarding information is essential to good government, maintaining the trust of the public and the workforce, and the quality and effectiveness of operations. In the Federal Personnel Vetting Guidelines, the Federal personnel vetting record and information sharing are addressed as critical personnel vetting elements. Departments and agencies must record personnel vetting determinations, to include investigative items and adjudicative information, in the government-wide repositories and internal systems, for increased mobility and transparency. Sharing information across and within departments and agencies eliminates unnecessary duplication and reduces waste.

Information sharing also improves transparency of the process, ensures quality, and maximizes efficiency. In the Common Principles in Applying Federal Personnel Vetting Adjudicative Standards, adjudicators are reminded of the responsibility to record personnel vetting actions and determinations because accurately reporting

this information promotes transparency, enhances mobility, and facilitates information sharing. This includes reporting reciprocal acceptance of determinations.

OPM is developing jointly with ODNI additional policy guidance for personnel vetting management that will be addressed to personnel vetting program practitioners at federal agencies. This policy will establish requirements for Executive Branch personnel vetting programs to apply sound risk management practices to assess the trustworthiness of individuals who work for or on behalf of the Federal government. With this policy, the Executive Agents can provide specific requirements for departments and agencies with respect to information sharing and can reemphasize the requirement for timely and accurate reporting.

I appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact Christine Bilunka at Christine.Bilunka@opm.gov.

Sincerely,

Lisa M. Loss
Suitability Director
U.S. Office of Personnel Management Suitability Executive Agent Programs

Attachment

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Alissa H. Czyz, (202) 512-3058 or CzyzA@gao.gov.

Staff Acknowledgments

In addition to the contact named above, Kimberly Seay (Assistant Director), James P. Klein (Analyst-in-Charge), Aaron Chua, Suellen Foth, Christopher Gezon, Kate Hu, Austin Lyke, Jared Michaels, Richard Powelson, Terry Richardson, Mike Shaughnessy, and Carter Stevens made key contributions to this report.

GAO's Mission

The Government Accountability 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 our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548