United States Government Accountability Office

Testimony

Before the Subcommittee on Government Operations and the Federal Workforce, Committee on Oversight and Accountability, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. ET
Wednesday, June 26, 2024

PERSONNEL VETTING

DOD Needs to Improve Management of the National Background Investigation Services Program

Statement of Alissa H. Czyz, Director, Defense Capabilities and Management

GAO-24-107616

June 2024

PERSONNEL VETTING

DOD Needs to Improve Management of the National Background Investigation Services Program

GAO Highlights

Highlights of GAO-24-107616, a testimony before the Subcommittee on Government Operations and the Federal Workforce, Committee on Oversight and Accountability, House of Representatives

Why GAO Did This Study

U.S. government personnel vetting processes, such as background investigations, rely on IT systems to process data on millions of federal employees and contractor personnel.

This statement summarizes information on (1) DCSA's progress in developing the NBIS system, (2) the reliability of the NBIS program schedule and cost estimate, and (3) DCSA's efforts to plan for cybersecurity and privacy controls for NBIS and legacy systems.

This statement is primarily based on published GAO reports since 2021 that have examined NBIS system development. To perform this work, GAO analyzed information on NBIS from DCSA and the Office of Personnel Management and interviewed knowledgeable officials about the NBIS program and NBIS and legacy systems.

What GAO Recommends

In the reports summarized in this statement, GAO made one Matter for Congressional Consideration on NBIS scheduling and cost estimating. It also made 15 recommendations to DOD to improve NBIS program management and cybersecurity. These recommendations have not yet been implemented. GAO continues to monitor their implementation status.

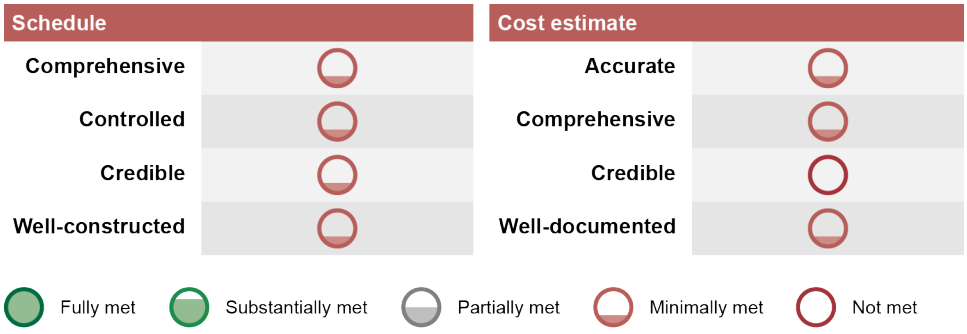
View GAO-24-107616. For more information, contact Alissa H. Czyz at (202) 512-3058 or czyza@gao.gov.

What GAO Found

The Department of Defense's (DOD) Defense Counterintelligence and Security Agency (DCSA) is developing a new information technology (IT) system—the National Background Investigation Services (NBIS)—for use in conducting background investigations for most federal agencies and over 13,000 organizations that work with the government. DCSA assumed responsibility for background investigation operations after two cybersecurity incidents in 2015 that compromised sensitive data from Office of Personnel Management systems on over 22 million federal employees and contractors. DCSA has developed some NBIS system capabilities to enhance the personnel vetting process, such as an eApplication that agencies and organizations will use to initiate the investigation process. However, DCSA has faced several delays in fully deploying NBIS, which was originally planned for 2019.

DCSA has repeatedly missed targeted milestones for fully deploying NBIS over the past several years, in part because DCSA does not yet have a reliable schedule and cost estimate for NBIS.

GAO's Prior Assessment of How NBIS's Schedule and Cost Estimate Have Met Best Practices



Source: GAO analysis of information for the National Background Investigation Services (NBIS) program. | GAO-24-107616

In 2021, GAO recommended that DCSA improve its schedule; after seeing a lack of progress, GAO recommended in 2023 that Congress consider requiring DCSA to do so. GAO also found that NBIS's 2022 cost estimate was not reliable. Given DOD's investment of over a half billion dollars in NBIS since 2016, developing a reliable schedule and cost estimate would improve program management and reduce the risk of cost overruns.

DCSA has also not fully planned for the cybersecurity controls needed to protect NBIS and legacy systems or fully implemented measures to manage privacy risks. For example, DCSA used an obsolete version of government-wide guidance to select the cybersecurity controls for six NBIS and legacy systems GAO reviewed. GAO recommended that DCSA address these gaps, as these systems may not be fully protected. In 2018, GAO placed the government-wide security clearance process on its High-Risk List due in part to challenges with IT systems.

Chairman Sessions, Ranking Member Mfume, and Members of the Subcommittee:

Thank you for the opportunity to be here today to discuss the Department of Defense's (DOD) development of the National Background Investigation Services (NBIS)—an information technology (IT) system intended for use in conducting background investigations for most federal agencies and over 13,000 organizations that work with the government.

Personnel vetting processes and the IT systems that support them are vital to determining the trustworthiness of the federal government's workforce and minimizing risks to U.S. national security. In 2015, two cybersecurity incidents compromised sensitive information in Office of Personnel Management (OPM) systems, including personnel vetting files, on over 22 million federal employees and contractors. A year later, the President assigned DOD the responsibility for developing and operating IT systems for personnel vetting processes.[1]

Today, DOD's Defense Counterintelligence and Security Agency (DCSA) is responsible for developing and securing the NBIS system for personnel vetting while also maintaining legacy IT systems.[2] Additionally, DCSA provides personnel vetting services for most of the government, including

[1]Specifically, in 2016, Executive Order No.13,467, as amended through Executive Order No. 13,741, assigned DOD the role of designing, developing, deploying, operating, securing, defending, and continuously updating and modernizing personnel vetting IT systems that support all background investigation processes that had been conducted by the National Background Investigations Bureau within the Office of Personnel Management. 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*, § 2.4(b)(June 30, 2008), as amended by Exec. Order No. 13,741, *Amending Executive Order 13467 To Establish the Roles and Responsibilities of the National Background Investigations Bureau and Related Matters*, § 1(f), 81 Fed. Reg. 68,289, 68,290 (Sept. 29, 2016).

[2]In this statement, the term "NBIS system" refers to the set of subsystems and associated capabilities that is the focus of the software development effort. The term "NBIS program" refers to the NBIS Program Management Office and its management of the program as a whole, including related subprojects such as acquisition, engineering, training, cybersecurity, etc.

conducting around 2 million background investigations each year.[3] DOD's continuing efforts to develop and deploy the NBIS system are occurring during the transition to Trusted Workforce 2.0, which is a major reform of the government's approach to personnel vetting.

Our work has covered DCSA's challenges in managing the development and cybersecurity of both NBIS and legacy IT systems.[4] We have made 15 recommendations intended to aid DCSA in its efforts to manage the NBIS program and have also pointed out issues that warrant congressional consideration.[5]

My testimony today addresses NBIS management and cybersecurity challenges. Specifically, I will focus on three key issues we identified in our reports: (1) DCSA's progress in developing the NBIS system, (2) the reliability of the NBIS program schedule and cost estimate, and (3) DCSA's efforts to plan for cybersecurity and privacy controls of selected NBIS and legacy systems.

This statement is based primarily on our reports issued from December 2021 through June 2024. In these reports, we also assessed other aspects of personnel vetting that have informed our updates on the government-wide personnel security clearance process—an issue on

[3]While DCSA conducts 95 percent of the government's background investigations, some executive branch agencies have the authority to conduct all or some of their own investigations, according to the Office of the Director of National Intelligence. Such agencies include the Central Intelligence Agency, the Federal Bureau of Investigation, and the State Department, as well as some DOD components such as the National Security Agency. According to OPM officials, OPM also delegates to DCSA and several other agencies the authority to conduct their own suitability, fitness, and credentialing investigations.

[4]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); *Personnel Vetting: Actions Needed to Implement Reforms, Address Challenges, and Improve Planning*, GAO-22-104093 (Washington, D.C.: Dec. 9, 2021); and *Personnel Vetting: DOD Needs to Enhance Cybersecurity of Background Investigation Systems,* GAO-24-106179 (Washington, D.C.: June 20, 2024).

[5]These recommendations have not yet been implemented and we continue to monitor their implementation.

GAO's High-Risk list.[6] To perform our prior work, we analyzed information on NBIS from DCSA and OPM. We also interviewed officials with knowledge of the NBIS program and NBIS and legacy systems. The reports we cite throughout this statement contain more details on the scope of our work and our methodologies.[7]

We conducted the work on which this statement is based in accordance with generally accepted government auditing standards. 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

The Personnel Vetting Process and Trusted Workforce 2.0

Personnel vetting processes help ensure the trustworthiness of the federal government's workforce and those who support it. Specifically, federal departments and agencies vet personnel to determine whether they are, and remain over time, (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.

The Security, Suitability, and Credentialing Performance Accountability Council (PAC) is responsible for the government-wide implementation of personnel vetting reforms and is involved in setting requirements for NBIS.[8] The PAC has four principal members: the Deputy Director for

[6]In 2018, we placed the government-wide security clearance process on our High-Risk List due in part to challenges with IT systems. In our latest High-Risk update, we found that the government-wide personnel security clearance process continues to face challenges with (1) the timely processing of clearances, (2) measuring the quality of investigations, and (3) IT systems. We have made numerous recommendations to address these challenges. For more information on our previous recommendations, see 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).

[7]We are also conducting a separate review of DCSA's implementation of cybersecurity controls for the NBIS system that will be published later in 2024 with limited distribution due to the sensitivity of the material covered.

[8]The PAC was established in June 2008 by Executive Order No. 13,467. *See* Exec. Order No. 13,467, § 2.2, 73 Fed. Reg. 38,103, 38,105 (June 30, 2008).

Management of the Office of Management and Budget (OMB); the Director of National Intelligence (DNI); the Director of OPM; and the Under Secretary of Defense for Intelligence and Security.

In March 2018, the PAC's principal members initiated Trusted Workforce 2.0 to reform the personnel vetting processes. The PAC provides publicly available quarterly updates on Trusted Workforce 2.0 on www.performance.gov. In April 2022, the PAC issued the *Trusted Workforce 2.0 Implementation Strategy*, 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. The PAC is incrementally implementing Trusted Workforce 2.0 and plans to fully implement the reform by fiscal year 2026.

DCSA and Background Investigation Services

Following the 2015 OPM cybersecurity incidents, DOD directed the Defense Information Systems Agency (DISA) to lead the acquisition of a new IT system to replace all OPM legacy IT systems supporting background investigation processes. DOD subsequently transferred the NBIS Program Management Office from DISA to DCSA on October 1, 2020. DCSA also took over the ownership and maintenance of OPM legacy systems and DOD legacy systems that support personnel vetting.[9] Figure 1 below shows a timeline of IT-related events for background investigations since 2015.

[9]OPM legacy systems include the Electronic Questionnaires for Investigations Processing (e-QIP). DOD also maintains its own legacy systems including Mirador, which is the DOD system of record for continuous vetting.

Figure 1: Timeline of Information Technology (IT)-Related Events since 2015 and DOD's Role in the Background Investigation Processes, as of August 2023

Source: GAO analysis of Office of Personnel Management (OPM) and Department of Defense (DOD) data. | GAO-24-107616

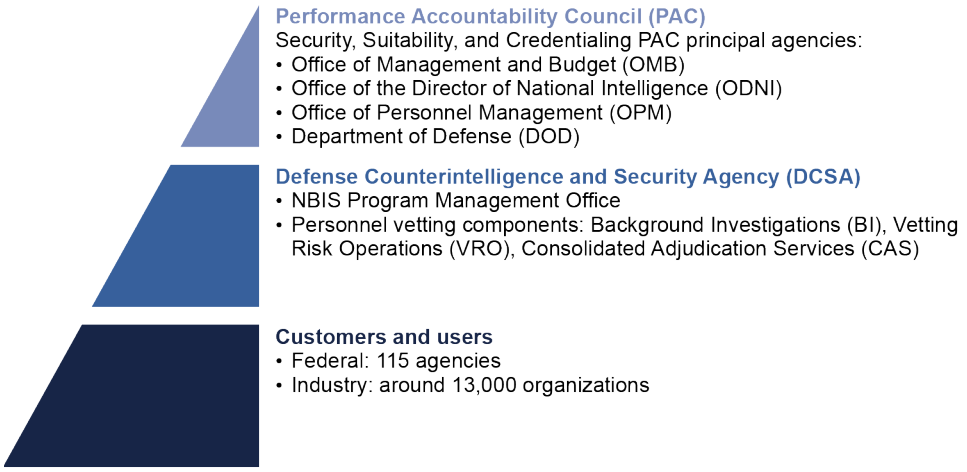
NBIS Program Management and Cost

DCSA's NBIS Program Management Office is responsible for maintaining, and eventually replacing, legacy IT systems that enable current background investigation processes to continue as it also delivers NBIS capabilities. NBIS program officials work directly with DCSA organizational components that carry out the agency's personnel vetting mission.[10] The NBIS program also engages with external organizations that use the NBIS system, including personnel security managers at more than 100 federal departments and agencies and over 13,000

[10]Within DCSA's organizational components, Background Investigations staff carry out around 2 million background investigations each year for the federal government. Consolidated Adjudication Services is the sole authority to determine security clearance eligibility of non-intelligence agency DOD personnel. Vetting Risk Operations leads the implementation of continuous vetting services.

organizations across the United States that work with the federal government (see fig. 2).

Figure 2: National Background Investigation Services (NBIS) Program Oversight, Program Management, and Stakeholder Organizations



Source: GAO analysis of DOD information. | GAO-24-107616

DOD initially spent around $654 million to develop the NBIS system from fiscal years 2017 through 2022, according to DOD budget justification documents.[11] The OPM legacy systems reside on OPM's network but are maintained by DOD personnel until those legacy systems are replaced by the NBIS system. As of August 2023, DOD had spent around $835 million to maintain these legacy systems from fiscal years 2020 through 2022 and planned to continue to fund the maintenance of OPM and DOD legacy systems for personnel vetting through fiscal year 2024.[12]

[11]Of this total amount for the NBIS program, DISA spent $430 million from fiscal years 2017 through 2020, and DCSA spent $223.5 million from fiscal years 2021 through 2022. This total is based on actual amounts in budget justification documents for research, testing, development, and evaluation (RDT&E) and operations and maintenance (O&M).

[12]DOD pays for the legacy systems by using two funding sources that originated from the transition of background investigation functions from OPM to DOD in 2019. First, DCSA established a working capital fund in June 2019 to finance personnel vetting activities, such as background investigations. Second, OPM transferred ownership of legacy IT systems to DCSA in October 2020, but they continue to reside on OPM's network. Under a series of interagency agreements, DCSA will continue to pay OPM for services associated with the legacy systems until they are replaced by the NBIS system.

In July 2023, we reported that starting in fiscal year 2024, DCSA planned to use its working capital fund to finance the NBIS program as well as its personnel vetting products (e.g., background investigations) and services (e.g., continuous vetting).[13] Working capital funds recover costs by charging customers a standard price for a product or service. For example, DCSA's continuous vetting services operate on a monthly subscription model and involve regularly reviewing a cleared individual's background to ensure the individual continues to meet security clearance requirements.

DCSA Has Developed and Deployed Various NBIS System Capabilities and Engaged with Stakeholders, but Delayed Milestones Have Hindered Progress

DCSA has deployed some NBIS system capabilities, such as an eApplication, to collect the necessary data to begin a background investigation. However, DCSA originally planned for NBIS to be fully operational in 2019 and it continues to miss milestones.

DCSA Has Developed and Deployed Some NBIS System Capabilities

In August 2023, we reported that DCSA's NBIS Program Management Office had successfully developed various NBIS system capabilities related to the key phases of the personnel vetting process.[14] Specifically, the program office has:

- **Deployed eApp**. DCSA fully deployed the eApplication (eApp) that most federal agencies and industry will use for personnel to complete the forms necessary to initiate the personnel vetting process.

[13]GAO, *Personnel Vetting: DOD Should Improve Management and Operation of Its Background Investigation Working Capital Fund,* GAO-23-105812 (Washington, D.C.: July 27, 2023). Working capital funds (WCFs) operate as self-supporting entities that conduct a regular cycle of businesslike activities and are designed to break even (i.e., not make profits or take losses) over the long term. Defense WCFs are designed to fully recover their costs over time through fees charged for products and services. The DCSA WCF recovers its costs by charging customers a standard price for each product or service.

[14]GAO-23-105670.

- **Delivered a tool for investigations**. DCSA delivered a position designation tool that assesses the duties and responsibilities of individual positions to determine the level of investigation required.
- **Developed an adjudication tool**. DCSA developed an NBIS data repository in which all federal departments and agencies that use NBIS will be expected to record the result of adjudications.
- **Developed capabilities for continuous vetting**. DCSA delivered initial capabilities for processing information from classified systems for continuous vetting.[15]

However, according to the April 2024 PAC quarterly update on Trusted Workforce 2.0, progress on certain milestones is delayed and contingent on the deployment of further NBIS capabilities. For NBIS to reach full implementation, federal agency and industry stakeholders must also adopt and scale the use of deployed capabilities within their own organizations. In August 2023, we reported that DCSA had almost completed its engagement with these stakeholders to provide them initial access and training on the system. In a survey on NBIS that we conducted, most federal and industry stakeholders that responded were generally satisfied with DCSA's engagement, initial training on eApp, and opportunities to provide feedback on the NBIS system. Nearly all of the federal and industry stakeholders that responded to our survey (55 of 60) said they had engaged with the DCSA team who reached out to them about the NBIS system, and nearly all of that group found that outreach to be useful.

DCSA Delays in Meeting Milestones Has Hindered Progress

DOD set up the NBIS program and began to develop the NBIS system in late 2016, but the program has encountered funding and policy changes and missed milestones that have delayed progress toward full implementation of NBIS capabilities. Under DISA management, DOD expected NBIS to reach full operational capability in 2019. NBIS officials then determined that those timeframes were unrealistic and created a

[15]Continuous vetting involves reviewing the background of a covered individual at any time to determine whether that individual continues to meet applicable requirements and allows for the replacement of traditional, time-based periodic reinvestigations. See Exec. Order No. 13,467, § 1.3(f), *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).

rebaselined program schedule.[16] This revised schedule remained in use as management of the program transferred from DISA to DCSA in October 2020.

Under DCSA's management, the program has continued to miss milestone dates for the delivery of capabilities. At the time of our review in August 2023, program officials attributed the delays to external circumstances, including a funding shortfall and the PAC issuing new Trusted Workforce policies that shifted NBIS program development priorities. For example, the NBIS program prioritized continuous vetting ahead of the deployment of background investigation capabilities, which shifted its milestone for those capabilities from September 2022 to March 2024.

Federal agency and industry stakeholders that responded to our 2023 survey developed as part of our review expressed concerns about delays in the full implementation of NBIS.[17] In response to our open-ended survey questions, 29 stakeholders responded that they had concerns with one or more elements of the transition process that needed to happen before NBIS could be used within their organizations. For example, eight stakeholders stated that using both the NBIS and legacy systems simultaneously could cause delays in processing applications. In addition, 10 stakeholders noted that they found the NBIS program milestones to be unrealistic, and they thought the status of NBIS system progress had been exaggerated.

In prior work, we reported that according to an official from the PAC Program Management Office, the most important factor in implementing Trusted Workforce 2.0 is DCSA's development of supporting IT systems like the NBIS system. Although DCSA has developed and deployed some NBIS system capabilities, it has faced continued delays in its full deployment of the system, which may in turn delay the successful

[16]DCSA officials refer to a revision of the NBIS program's milestones as "rebaselining." A program's baseline schedule is used to manage the scope of the program and the time and resources required to accomplish tasks. Rebaselining can occur if management concludes that the remaining schedule target for completing a program is insufficient and that the current baseline is no longer valid for realistic performance measurement. *See* GAO, *Schedule Assessment Guide: Best Practices for Project Schedules*, GAO-16-89G (Washington, D.C.: Dec. 22, 2015).

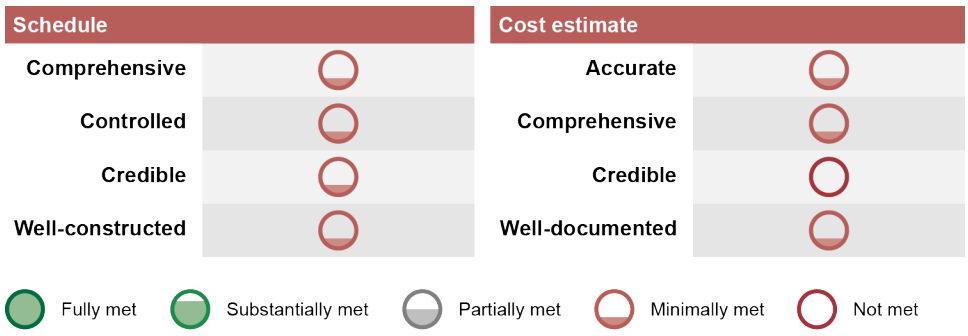
[17]In August 2023, we recommended that DOD assess and use our survey results to inform its efforts to improve engagement with federal government and industry stakeholders. DOD concurred with the recommendation and identified steps it planned to take to implement it. GAO-23-105670.

implementation of Trusted Workforce 2.0 reforms. For example, in fiscal year 2024, the PAC reported that DCSA missed its target to transition continuous vetting customers to Trusted Workforce 1.5 by December 2023 because meeting that milestone was contingent on NBIS capabilities. According to the PAC program management office, DOD is reviewing its Integrated Master Schedule for NBIS in response to our recommendations, and several major milestones for Trusted Workforce 2.0 are being pushed out to reflect the most recent state of NBIS development.

DOD Does Not Yet Have a Reliable Schedule or Cost Estimate to Manage the NBIS Program

DOD's lack of progress in addressing NBIS schedule weaknesses we identified in 2021 and 2023 could further delay system implementation and the planned replacement of legacy systems. In addition, we found that the NBIS program's cost estimate from 2022 was not reliable. The success of the NBIS program depends, in part, on having a reliable schedule that defines when and how long work will occur and a realistic estimate of projected costs. Figure 3 summarizes our analysis of DCSA's schedule and cost estimate.

Figure 3: GAO's Prior Assessment of How NBIS's Schedule and Cost Estimate Have Met Best Practices



Source: GAO analysis of information for the National Background Investigation Services (NBIS) program. | GAO-24-107616

Note: We assessed the Defense Counterintelligence and Security Agency's (DCSA) schedule files as of February 2023 for the National Background Investigation Services (NBIS) program against industry best practices for developing a schedule published in the GAO *Schedule Assessment Guide*. A high-quality, reliable schedule has four characteristics: it is comprehensive, controlled, credible, and well-constructed. We assessed DCSA's cost estimate from 2022 for the NBIS program against best practices for cost estimating published in the GAO *Cost Estimating and Assessment Guide*. A high-quality cost estimate has four characteristics: it is accurate, comprehensive, credible, and well-documented. These best practices are also referenced in the GAO *Agile Assessment Guide*.

As of August 2023, DOD had not resolved weaknesses in the NBIS schedule that we first identified in 2021. We found in both 2021 and 2023

that the NBIS schedule did not substantially meet any of the four characteristics of reliable schedules as defined in GAO's *Schedule Assessment Guide* and *Agile Assessment Guide*.[18] Specifically, the guides provide that schedules must be comprehensive, controlled, credible, and well-constructed. For example, we were unable to confirm whether the schedule tracks all key deliverables. We also could not trace the sequence of activities that would determine the program's earliest completion date, a potential limitation on management's ability to provide reliable timelines. An unreliable schedule may prevent DCSA management from effectively guiding the delivery and continued maintenance of personnel vetting capabilities for the federal government and industry.

In 2021, DOD concurred with our recommendation to revise the NBIS program schedule to meet best practices, but the extent to which program management has prioritized schedule development was unclear. NBIS program officials have stated that the benefit of using a schedule must outweigh the effort to implement it and that onerous, non-critical, administrative burdens are a secondary priority for the program. However, the NBIS program already employs staff to update the schedule and, according to the GAO *Agile Assessment Guide*, schedules for software programs should contain enough detail so that updates are not overly frequent or cumbersome. Program officials also stated that the current NBIS schedule follows DOD's guidance on the software acquisition pathway, but this guidance does not detail how to develop or maintain a schedule.[19]

Given the lack of progress in improving the reliability of the NBIS system implementation schedule as of August 2023, we recommended that Congress consider requiring the NBIS Program Management Office to

[18]GAO considers a schedule to be reliable if the assessment ratings for each of the four characteristics are substantially met or fully met. If any of the characteristics are rated as not met, minimally met, or partially met, then the schedule cannot be considered reliable. GAO, *Schedule Assessment Guide: Best Practices for Project Schedules*, GAO-16-89G (Washington, D.C.: Dec. 22, 2015); and *Agile Assessment Guide: Best Practices for Agile Adoption and Implementation*, GAO-20-590G (Washington, D.C.: September 2020).

[19]In 2020, DOD established six acquisition pathways—or sets of policy and guidance—that are tailored to the type of capabilities being acquired. DOD requires programs on its software pathway to use requirements processes tailored to support Agile development. For example, software pathway programs are to use streamlined requirements documents and develop user agreements, which help ensure programs iteratively develop software aligned with user needs. *See* GAO, *Defense Software Acquisitions: Changes to Requirements, Oversight, and Tools Needed for Weapon Programs*, GAO-23-105867 (Washington, D.C.: July 20, 2023).

develop a reliable program implementation schedule. As of March 2024, DOD stated it would complete actions to revise the NBIS schedule by the end of fiscal year 2024 and it conducted an analysis that identified actions to improve the schedule. Until DOD addresses the reliability of the NBIS schedule, NBIS implementation and the planned replacement of legacy systems could be further delayed.

The NBIS Cost Estimate Is Not Reliable

In August 2023, we reviewed the NBIS program's 2022 cost estimate and found that it was not reliable because it did not substantially meet any of the four characteristics of a reliable cost estimate, as defined in GAO's *Cost Estimating and Assessment Guide* and *Agile Assessment Guide* and shown in figure 3 above.[20] The estimate we reviewed totaled $767.9 million for fiscal years 2023 through 2027. However, we found that the estimate, among other issues, did not reflect actual costs and that the supporting documentation discussed some, but not all, ground rules and assumptions that could invalidate the estimate if any were rejected by management.

At the time of our review, NBIS program officials noted that cost estimating had been challenging. They provided several reasons why the cost estimate they had developed did not meet our best practices, including because DOD guidance does not require certain kinds of documentation and the program faced resource limitations. They pointed out that the program had not experienced significant cost overruns. However, DCSA may be unable to effectively project NBIS costs with an unreliable cost estimate. We recommended that Congress consider requiring the NBIS Program Management Office to develop a reliable cost estimate because it is especially critical as DCSA begins to rely on the system to provide services to the rest of the government. DOD implementation of our best practices for cost estimating would help Congress better ensure that DOD is collecting the data necessary to

[20]All best practices need to be at least substantially met for a schedule or cost estimate to be considered reliable. These characteristics also apply to Agile programs, which have dynamic and iterative processes and spread planning activities throughout the program's duration. GAO, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Program Costs*, GAO-20-195G (Washington, D.C.: Mar. 12, 2020); and *Agile Assessment Guide*, GAO-20-590G.

prevent cost increases or delays in delivering services through NBIS that are necessary to implement Trusted Workforce 2.0.[21]

DCSA Needs to Strengthen Cybersecurity and Privacy Controls of Selected NBIS and Legacy Systems

The 2015 breaches of OPM legacy systems demonstrated the damage that increasingly sophisticated cyber threats can cause. In response, DOD began developing NBIS to replace the legacy systems and, until NBIS is deployed, DCSA continues to use these legacy systems. However, earlier this month, we reported that DCSA has not fully planned for the cybersecurity controls needed to protect NBIS and legacy systems or fully implemented privacy controls.[22] For example, we found the following:

- DCSA did not fully define and prioritize requirements to ensure cybersecurity and privacy in the six systems we reviewed. For example, DCSA identified the privacy requirements for four of the systems. However, documentation for the two remaining systems were either incomplete or lacked documentation of review and approval by a senior official.[23]
- DCSA used an obsolete version of government-wide guidance to select the cybersecurity controls for the six NBIS and legacy systems we reviewed.[24]
- DCSA did not fully implement controls to manage privacy risks for the six systems we reviewed.[25] For example, while we found that all

[21]According to DCSA, it planned to use its working capital fund starting in fiscal year 2024 to finance the NBIS program as well as its products (e.g., background investigations) and services (e.g., continuous vetting).

[22]GAO, *Personnel Vetting: DOD Needs to Enhance Cybersecurity of Background Investigation Systems*, GAO-24-106179 (Washington, D.C.: June 20, 2024).

[23]DCSA identified seven NBIS and 11 legacy systems. From these, we selected six systems for our review—three NBIS systems and three legacy systems previously owned by OPM. We selected these systems because they process, store, and transmit large amounts of sensitive data, are critical to DCSA's personnel vetting operations, and are currently authorized to operate. We do not name the six systems in relation to any assessment results because this information is considered controlled unclassified information and is not authorized for public release.

[24]Cybersecurity controls are safeguards or countermeasures prescribed for an information system or an organization. These controls are designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

[25]Privacy controls are safeguards employed within an agency to ensure compliance with privacy requirements and manage privacy risks.

sampled users of these six systems had completed security training, DCSA had not ensured that all training and certifications were current.

- DCSA had not established an oversight process to ensure that it completes all required cybersecurity planning and provide visibility to remedy gaps in privacy controls in NBIS and legacy systems.

We made 13 recommendations to DOD to address the cybersecurity and privacy shortfalls we reported. DOD concurred with 12 of our recommendations and did not concur with one recommendation. DOD officials stated that the department is taking action to address the shortfalls we identified. Until DCSA fully implements our recommendations, including establishing an oversight process to enable DCSA's Chief Information Officer to address cybersecurity planning and providing visibility into the implementation of privacy controls, NBIS and legacy systems may not be fully protected.

In summary, although DCSA has put in place some NBIS system capabilities, full deployment of the system is years behind original plans, and DCSA lacks a reliable schedule and cost estimate that would help reduce the risk of continued delays and potential cost overruns. In addition, DCSA needs to address issues related to cybersecurity planning and privacy controls of both NBIS and legacy systems. Implementing our recommendations in these areas could help DOD avoid further delays to the full implementation of NBIS and personnel vetting reform generally. Implementing these recommendations could also help DCSA ensure its ability to properly manage and mitigate security risks for all background investigation systems presently and in the future.

Chairman Sessions, Ranking Member Mfume, and Members of the Subcommittee, this concludes my prepared statement. I would be pleased to respond to any questions you may have at this time.

GAO Contact and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact Alissa H. Czyz, Director, Defense Capabilities and Management, 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 statement. GAO staff who made key contributions to this testimony are James P. Klein and Kimberly Seay (Assistant Directors), Parke Nicholson (Analyst-in-Charge), Megan Condon, Jennifer Franks, Ashley Houston, Amie Lesser, Kelly Liptan, Matthew Luciano, Andrew Stavisky, Carter Stevens, Daniel Swartz, and Lillian Moyano Yob.

Related GAO Products

Personnel Vetting: DOD Needs to Enhance Cybersecurity of Background Investigation Systems. GAO-24-106179. Washington, D.C.: June 20, 2024.

Federal Workforce: Actions Needed to Improve the Transfer of Personnel Security Clearances and Other Vetting Determinations. GAO-24-105669. Washington, D.C.: January 22, 2024.

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

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.: April 20, 2023.

Personnel Vetting: Actions Needed to Implement Reforms, Address Challenges, and Improve Planning. GAO-22-104093. Washington, D.C.: December 9, 2021.

High Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas. GAO-21-119SP. Washington, D.C.: March 2, 2021.

Federal Management: Selected Reforms Could Be Strengthened by Following Additional Planning, Communication, and Leadership Practices. GAO-20-322. Washington, D.C.: April 23, 2020.

High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas. GAO-19-157SP. Washington, D.C.: March 6, 2019.

Personnel Security Clearances: Additional Actions Needed to Implement Key Reforms and Improve Timely Processing of Investigations. GAO-18-431T. Washington, D.C.: March 7, 2018.

Personnel Security Clearances: Additional Actions Needed to Ensure Quality, Address Timeliness, and Reduce Investigation Backlog. GAO-18-29. Washington, D.C.: December 12, 2017.

Personnel Security Clearances: Plans Needed to Fully Implement and Oversee Continuous Evaluation of Clearance Holders. GAO-18-117. Washington, D.C.: November 21, 2017.

Information Security: OPM Has Improved Controls, but Further Efforts Are Needed. GAO-17-614. Washington, D.C.: August 3, 2017.

Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems. GAO-16-501. Washington, D.C.: May 18, 2016.