United States Government Accountability Office

Report to Congressional Committees

June 2024

PERSONNEL VETTING

DOD Needs to Enhance Cybersecurity of Background Investigation Systems

GAO-24-106179

GAO Highlights

Highlights of GAO-24-106179, a report to congressional committees

June 2024

PERSONNEL VETTING

DOD Needs to Enhance Cybersecurity of Background Investigation Systems

Why GAO Did This Study

In the wake of a 2015 OPM breach that compromised sensitive data on over 22 million federal employees and contractors, DCSA later assumed responsibility for conducting background investigation operations for most executive branch agencies.

House Report 117-118 includes a provision for GAO to evaluate the cybersecurity of DCSA's background investigation systems. GAO assessed the extent to which DCSA (1) planned for cybersecurity controls for selected background investigation systems and (2) implemented privacy controls for these systems.

GAO selected three DCSA systems and three OPM legacy systems critical to background investigation operations. GAO (1) reviewed policies, processes, and documentation for these systems and (2) interviewed agency officials regarding the planning and management of cybersecurity risks and selected privacy controls. GAO also has ongoing work assessing DCSA's implementation of technical controls for background investigation systems. It will be published in a future report with limited distribution.

What GAO Recommends

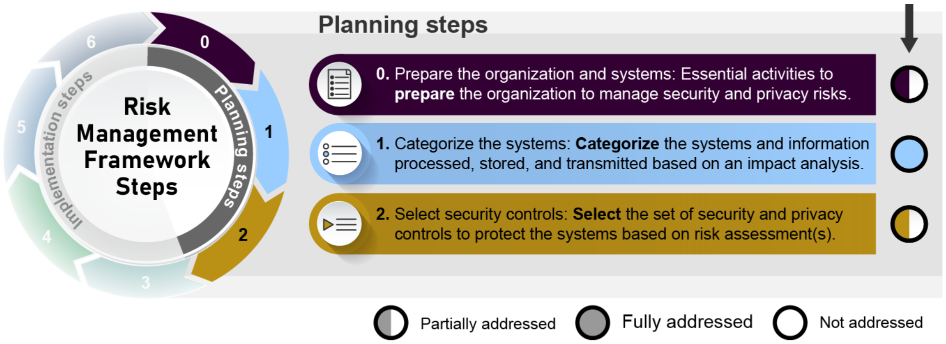
GAO is making a total of 13 recommendations to DOD on fully implementing risk management planning steps, selecting appropriate security controls using current guidance, fully implementing privacy controls, and establishing oversight processes to help ensure required tasks and controls are implemented. DOD concurred with 12 of 13 recommendations and non-concurred with one. GAO maintains that all recommendations are warranted.

View GAO-24-106179. For more information, contact Jennifer R. Franks at (404) 679-1831 or franksj@gao.gov and Alissa H. Czyz, (202) 512-3058 or czyza@gao.gov.

What GAO Found

To conduct background investigations, the Department of Defense's (DOD) Defense Counterintelligence and Security Agency (DCSA) currently uses a combination of recently developed DOD National Background Investigation Services systems and legacy systems formerly owned by the Office of Personnel Management (OPM). In considering the cybersecurity risks of these systems, DCSA did not fully address all planning steps of DOD's risk management framework (see figure).

Extent to Which Defense Counterintelligence and Security Agency Addressed DOD's Planning-Related Risk Management Steps for Selected Background Investigation Systems as of December 2023



0. Prepare the organization and systems: Essential activities to **prepare** the organization to manage security and privacy risks. ◐

1. Categorize the systems: **Categorize** the systems and information processed, stored, and transmitted based on an impact analysis. ●

2. Select security controls: **Select** the set of security and privacy controls to protect the systems based on risk assessment(s). ◐

◐ Partially addressed ● Fully addressed ○ Not addressed

Sources: GAO (icons and analysis of Department of Defense [DOD] guidance); colorlife/stock.adobe.com (illustration). | GAO-24-106179

Note: DOD's implementation-related Risk Management Steps are to (3) establish an implementation approach, (4) assess security controls, (5) authorize the systems, and (6) monitor security controls.

- **Prepare the organization and systems:** Of the 16 tasks required by this step in DOD's risk management framework, DCSA fully addressed 11, partially addressed two, and did not address three. For example, the agency has not fully defined and prioritized security and privacy requirements, nor has it performed organizational and system-level risk assessments.
- **Categorize the systems:** DCSA appropriately categorized the six reviewed systems as high impact risks**.**
- **Select security controls:** DCSA selected baseline security controls for the six systems but used an outdated version of government-wide guidance as the source for the control selections. Specifically, version five of applicable National Institute for Standards and Technology guidance was issued in 2020. However, DCSA continues to use version four. Among the changes in version five are two new categories of controls on personally identifiable information and supply chain management, raising the number of control categories from 18 to 20.

Regarding privacy, DCSA partially implemented controls on developing policies and procedures, delivering training, defining and reviewing the types of events to log, and assessing controls and risks. The agency lacks an oversight process to help ensure that appropriate privacy controls are fully implemented. Until DCSA establishes such an oversight process and fully implements privacy controls, it unnecessarily increases the risks of disclosure, alteration, or loss of sensitive information on its background investigation systems.

Contents

Letter 1

Background 5

DCSA Has Not Fully Planned for the Cybersecurity of NBIS and Legacy Systems 12

DCSA Did Not Fully Implement Privacy Controls for Selected Background Investigation Systems 18

Conclusions 25

Recommendations for Executive Action 26

Agency Comments and Our Evaluation 28

Appendix I Objectives, Scope, and Methodology 31

Appendix II Comments from the Department of Defense 36

Appendix III Contacts and Staff Acknowledgments 42

Tables

Table 1: Extent to Which DCSA Policies and Practices Addressed Required Tasks in the *Prepare* Step of DOD's Risk Management Framework at the Organization and System Levels 12

Table 2: DCSA-Assigned Impact Levels for the Six Selected Background Investigation Systems 16

Table 3: Control Areas and Privacy Controls for Selected Background Investigation Systems 18

Table 4: Selected NBIS and Legacy Background Investigation Systems 31

Table 5: Summary of Selected Privacy Controls for National Background Investigation Services and Legacy Background Investigation Systems 34

Figure

Figure 1: Overview of DOD's Cybersecurity Risk Management Framework Steps for IT Systems 10

Abbreviations

CIO	chief information officer
DCSA	Defense Counterintelligence and Security Agency
DISA	Defense Information Systems Agency
DOD	Department of Defense
IT	information technology
NBIS	National Background Investigation Services
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OPM	Office of Personnel Management

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

June 20, 2024

The Honorable Mark Warner
Chairman
The Honorable Marco Rubio
Vice Chairman
Select Committee on Intelligence
United States Senate

The Honorable Mike Rogers
Chairman
The Honorable Adam Smith
Ranking Member
Committee on Armed Services
House of Representatives

Personnel vetting processes are vital to determining the trustworthiness of the federal government's workforce by minimizing risks from personnel not suitable for government employment. Having robust vetting processes and securing the information systems used in those processes help prevent unauthorized disclosure of classified and sensitive information that could damage U.S. national security.

In 2015, two cybersecurity incidents compromised sensitive information in Office of Personnel Management (OPM) systems that contained personnel records and background investigation information. These breaches exposed sensitive information, including security clearance files, on over 22 million federal employees and contractors. These cyber incidents demonstrated the damage that increasingly sophisticated cyber threats can cause, particularly cyber threats originating from foreign adversaries. Improving the security of systems used for personnel vetting is imperative to protecting the confidentiality, integrity, and availability of the information on federal systems, including personally identifiable information.[1]

Following the 2015 incidents, the President assigned the Department of Defense (DOD) the responsibility for developing and operating IT systems for all personnel vetting processes. In response to the President's

[1] Personally identifiable information includes information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, mother's maiden name, biometric records, or any other personal information that is linkable to an individual.

directive, DOD set up the National Background Investigation Services (NBIS) Program Executive Office in late 2016 and started developing the NBIS system as a replacement for a suite of legacy IT systems.[2]

In 2019, DOD established the Defense Counterintelligence and Security Agency (DCSA), which among other things, assumed responsibility from OPM for conducting background investigation operations for most executive branch agencies.[3] DCSA also assumed responsibility for the NBIS Program Executive Office and inherited the NBIS program. DCSA is now the federal government's primary investigative service provider and conducts more than 95 percent of the government's background investigations.[4]

House Report 117-118, accompanying H.R. 4350, the House-passed version of the National Defense Authorization Act for Fiscal Year 2022, includes a provision for us to review the NBIS system.[5] Our objectives were to assess the extent to which DCSA (1) planned for cybersecurity controls for the NBIS system and legacy background investigation systems (hereinafter referred to as legacy systems) and (2) implemented

[2] In this report, we use the term "NBIS system" to refer to the set of subsystems and associated capabilities that is the focus of the software development effort. The term "NBIS program" refers to the program as a whole. This encompasses the NBIS Program Executive Office's management of related subprojects such as acquisition, engineering, training, and cybersecurity. Legacy background investigation systems are the set of systems formerly operated by OPM for personnel vetting that will be replaced by NBIS.

[3] See The White House, *Transferring Responsibility for Background Investigations to the Department of Defense*, Executive Order No. 13869 (Apr. 19, 2019) (amending Executive Order No.13467 of June 30, 2008). Section 925 of the National Defense Authorization Act for Fiscal Year 2018 generally resulted in the transfer of background investigations from OPM to DOD for DOD personnel. See Pub. L. No. 115-91, § 925(a)-(d), 131 Stat. 1283, 1526-27 (2017). In addition to implementing section 925, Exec. Order 13869 transferred responsibility to DCSA for conducting national security background investigations for most other executive branch agencies. It further facilitated the delegation of responsibility for suitability and fitness background investigations for most non-DOD agencies from OPM to DCSA. See Exec. Order 13869, §§ 1, 2 (amending section 2.6 of Exec. Order 13467).

[4] 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 including the National Security Agency.

[5] H.R. Rep. No. 117-118, National Defense Authorization Act for Fiscal Year 2022, at 220-21 (2021), accompanying H.R. 4350, 117th Cong. 1st Sess. (2021).

privacy controls for these systems.[6] This report builds on work in our August 2023 NBIS report.[7] We are conducting a separate review of DCSA's implementation of cybersecurity controls for the NBIS system that we expect to complete in 2024.[8]

Among the seven NBIS and 11 legacy systems DCSA identified, we selected six systems for our review—three NBIS 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.[9]

To determine the extent to which DCSA planned for cybersecurity controls for the selected systems, we reviewed DOD's instruction on cybersecurity risk management (also referred to as the DOD Risk Management Framework) and identified seven risk management steps.[10] From these, we selected three risk management steps we deemed critical for the planning of cybersecurity: prepare the organization and systems, categorize the systems, and select security controls.

Next, we analyzed documentation related to DCSA's planning and implementation efforts at the organizational and system levels for each selected system's program office (e.g., policies, procedures, system security plans, system categorization results, and privacy impact assessments). We evaluated this documentation against the three

[6] Cybersecurity controls are safeguards or countermeasures prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements. Privacy controls are safeguards employed within an agency to ensure compliance with privacy requirements and manage privacy risks.

[7] See 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).

[8] Our ongoing work related to DCSA's implementation of cybersecurity controls for the NBIS system will be published in a subsequent report with limited distribution due to the sensitivity of the material covered.

[9] We do not name the six systems in relation to any assessment results. This information is considered controlled unclassified information and is not authorized for public release.

[10] Department of Defense, Office of the Chief Information Officer, *DOD Risk Management Framework (RMF) for Information Technology (IT),* DOD Instruction 8510.01 (July 19, 2022).

selected risk management planning steps,[11] the National Institute of Standards and Technology's (NIST) risk management framework,[12] and National Security Agency (NSA) security control guidance.[13]

Additionally, we interviewed relevant DCSA officials about their efforts to manage and oversee the cybersecurity for their respective systems to determine the extent to which each system's program office had addressed the selected risk management steps.

To assess the implementation of privacy controls for the selected NBIS and legacy systems, we reviewed NIST Special Publication 800-53 Revision 5 to identify the baseline controls for protecting an individual's privacy.[14] We selected eight privacy controls related to the following areas: (1) developing policies and procedures, (2) delivering training, (3) establishing event logging protocols, and (4) assessing selected controls and system risks. We reviewed and analyzed documents used by DCSA officials responsible for the six systems to implement, oversee, and demonstrate compliance with these eight selected privacy controls. We evaluated this documentation against NIST guidance for the eight controls.

For the training controls, we selected a random sample of personnel with direct access to NBIS systems to estimate the population percentage of personnel that received security training. Additionally, we identified the

[11] Where available, DCSA provided system categorization results, system security plans, security assessment reports, authorizations to operate documentation, corrective action plans, and the system-level continuous monitoring strategies as evidence of its efforts.

[12] National Institute of Standards and Technology (NIST), *Assessing Security and Privacy Controls in Information Systems and Organizations,* Special Publication 800-53A, Rev. 5 (Gaithersburg, Md.: Jan. 2022); *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, Rev. 5 (Gaithersburg, Md.: Sept. 2020); and *Risk Management Framework for Information Systems and Organizations*, Special Publication 800-37, Rev. 2 (Gaithersburg, Md.: Dec. 2018).

[13] National Security Agency, Committee on National Security Systems (CNSS) Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems,* (Fort Meade, Md.: July 2022). Although the six systems in this report are critical to DCSA's personnel vetting operations, these systems are not considered national security systems as defined in 44 U.S.C. § 3552(b)(6)(A). Nevertheless, DOD Instruction 8510.01 requires that programs for all systems categorize and select controls—the first two steps in the DOD risk management framework—in accordance with guidance from the Committee on National Security Systems Instruction No. 1253. This guidance builds on and is a companion document to NIST guidance relevant to categorization and selection.

[14] National Institute of Standards and Technology, Special Publication 800-53, Rev. 5 identifies security and privacy controls that organizations can use to protect their systems.

personnel in our sample with privileged access to NBIS systems to determine how many of them had received required privileged user training. Because the sample was not made based on privileged access, the privileged user training result is nongeneralizable.

We supplemented our analysis of documents and data by interviewing officials in DCSA's Office of the Chief Information Officer and the system program offices about their efforts to implement, assess, document, and review selected privacy control tasks for their respective systems. A detailed discussion of our objectives, scope, and methodology can be found in appendix I.

We conducted this performance audit from August 2022 to June 2024 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 Security, Suitability, and Credentialing Performance Accountability Council is responsible for driving the implementation of security clearance reforms.[15] The council has four principal members: the Deputy Director for Management of the Office of Management and Budget, the Director of National Intelligence, the Director of OPM, and the Under Secretary of Defense for Intelligence and Security.

[15] The White House, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contract Employees, and Eligibility for Access to Classified National Security Information,* Executive Order No. 13467, § 2.2 (June 30, 2008). This order established the Suitability and Security Clearance Performance Accountability Council, now referred to as the Security, Suitability, and Credentialing Performance Accountability Council.

Personnel vetting is a detailed assessment of an individual to determine suitability, fitness, and eligibility. Personnel vetting can also provide credentials for that individual to hold a national security clearance, to access classified information, or to hold a sensitive position.

Continuous vetting is a process where a cleared individual’s background is regularly reviewed to ensure the individual continues to meet security requirements and should continue to hold trusted positions or credentials.

The goal of vetting is to minimize the risk to the nation from personnel not being suitable for government employment, to ensure personnel have the proper credentials to access facilities, or to prevent unauthorized disclosure of information that could damage national security.

Source: GAO summary of Performance Accountability Council and Defense Counterintelligence and Security Agency information. | GAO-24-106179

In March 2018, the Security, Suitability, and Credentialing Performance Accountability Council announced a government-wide initiative to fundamentally overhaul the federal personnel vetting process through a series of policy and procedural reforms called Trusted Workforce 2.0. The initiative aims to reduce the time to bring new hires onboard, enable mobility of the federal workforce, and improve insight into workforce behaviors while mitigating risk. The council divided implementation of this initiative into two phases: (1) reduce and eliminate the backlog of background investigations conducted by DCSA and (2) establish a new government-wide approach to personnel vetting.

As we reported in 2021, the Security, Suitability, and Credentialing Performance Accountability Council has made progress in implementing both phases.[16] This includes requiring federal agencies to adopt continuous vetting in two interim phases—Trusted Workforce 1.25 and 1.5.[17] In 2022, the council issued other key Trusted Workforce 2.0 policies, including updated investigative standards that also address continuous vetting.[18]

DCSA and Background Investigation Services

According to the Security, Suitability, and Credentialing Performance Accountability Council, the most important factor in implementing Trusted Workforce 2.0 is DCSA’s development of supporting IT systems. 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. In 2016, DISA established the NBIS Program Management Office and, according to DOD, awarded an “other

[16] GAO, *Personnel Vetting: Actions Needed to Implement Reforms, Address Challenges, and Improve Planning,* GAO-22-104093 (Washington, D.C.: Dec. 9, 2021). According to Security, Suitability, and Credentialing Performance Accountability Council documentation, DCSA has eliminated its backlog and maintained its target inventory since the third quarter of fiscal year 2021.

[17] See Office of the Director of National Intelligence and Office of Personnel Management, *Transforming Federal Personnel Vetting: Continuous Vetting and Other Measures to Expedite Reform and Transition to Trusted Workforce 2.0* (Jan. 15, 2021) and *Transforming Federal Personnel Vetting: Measures to Expedite Reform and Further Reduce the Federal Government’s Background Investigation Inventory* (Feb. 3, 2020). DCSA has provided a Trusted Workforce 1.25 service to provide for automated record checks in several data categories and is transitioning customer agencies to a service that meets Trusted Workforce 1.5 requirements. Trusted Workforce 1.5 requirements include automated record checks in data categories such as eligibility, terrorism, foreign travel, suspicious financial activity, criminal activity, credit, and commercial data.

[18] See Office of the Director of National Intelligence and Office of Personnel Management, *Federal Personnel Vetting Investigative Standards* (May 17, 2022).

transaction agreement" (a contracting mechanism) in 2018 to develop NBIS.[19]

In 2019, DOD later established DCSA to assume responsibility from OPM for conducting national security background investigations for most executive branch agencies.[20] 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's legacy systems on that date.

Overview of NBIS and Legacy Systems

Legacy background investigation systems are the set of systems formerly operated by the Office of Personnel Management (OPM) for personnel vetting that will be replaced by the National Background Investigation Services (NBIS) system. According to agency officials, these systems are currently operated by DCSA but continue to reside on OPM's network. DCSA plans to incrementally decommission these legacy systems as NBIS capabilities are deployed to replace them. Currently, projected decommissioning of all legacy systems is the end of 2024.

Source: GAO analysis of Defense Counterintelligence and Security Agency (DCSA) information. | GAO-24-106179

The NBIS systems' capabilities, once fully deployed, are to include a range of software tools and data repositories to enable personnel vetting.[21] These capabilities include the completion of electronic forms by individuals who are subject to personnel vetting, investigation management, subject management, the recording of background investigation adjudication decisions, and continuous vetting. The capabilities also include other processes related to managing the background investigation records of federal employees, military personnel, and contractors. The government's full implementation of NBIS system capabilities should enable the transition from legacy personnel vetting systems and the incremental decommissioning of those legacy systems.[22] According to agency officials, although these systems are currently operated by DCSA, they continue to reside on OPM's network throughout the decommissioning process. DCSA projects that all legacy systems will be decommissioned by the end of 2024. However,

[19] DISA stated it used an "other transaction agreement" for NBIS development to acquire leading-edge technologies by tapping into a nontraditional defense contractor base and to engage industry for a broad range of research and prototyping activities.

[20] See The White House, Exec. Order 13869. Section 925 of the National Defense Authorization Act for Fiscal Year 2018 generally resulted in the transfer of background investigations from OPM to DOD for DOD personnel. See Pub. L. No. 115-91, § 925(a)-(d), 131 Stat. 1283, 1526-27 (2017). In addition to implementing section 925, Exec. Order 13869 transferred responsibility to DCSA for conducting national security background investigations for most other executive branch agencies. It further facilitated the delegation of responsibility for suitability and fitness background investigations for most non-DOD agencies from OPM to DCSA. See Exec. Order 13869, §§ 1, 2 (amending section 2.6 Exec. Order 13467).

[21] According to NBIS program documentation, the program will have fully deployed a NBIS capability after delivering a complete set of code for one of the four phases of personnel vetting (initiation, investigation, adjudication, and continuous vetting).

[22] According to the NBIS program, decommissioning means the termination of a legacy system's operations. The system is turned off and personnel are no longer needed to maintain the applications and data on the system.

according to DCSA's decommissioning plan, the legacy systems will contain sensitive information requiring safeguarding until certain steps in the decommissioning process are complete.

Cybersecurity Risk Management

Cybersecurity risk management comprises a full range of activities undertaken to protect IT systems and data from cyber threats such as unauthorized access. This involves maintaining awareness of these threats, as well as detecting anomalies and incidents adversely affecting IT systems and data. Additionally, risk management includes responding to and recovering from cybersecurity incidents and mitigating their impact.

A **cybersecurity threat** is anything that can potentially harm a system, either intentionally or unintentionally.

Source: GAO summary of National Institute of Standards and Technology information. | GAO-24-106179

Federal law and guidance specify requirements for protecting federal information and information systems. Specifically, the Federal Information Security Modernization Act of 2014 requires executive branch agencies to develop, document, and implement agency-wide programs to provide security for the information and information systems that support their mission.[23] NIST was tasked with developing standards and guidelines for agencies to use in establishing minimum cybersecurity requirements for such information and information systems based on their respective levels of cybersecurity risk.[24] Accordingly, NIST developed a risk management framework to improve information security and strengthen risk management processes, among other things.[25] NIST also developed a catalog of security and privacy controls to protect agency information systems.[26]

DOD's Office of the Chief Information Officer (CIO) has also established policies, procedures, and guidance to help defend its information systems and computer networks. These include the *Risk Management Framework for DOD Systems* (DOD Instruction 8510.01), which describes the department's requirements for executing and maintaining the risk

[23] 44 U.S.C. § 3554(b). The Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (2014), updated and largely superseded the Federal Information Security Management Act of 2002, Pub. L. No. 107-347, Title III, 116 Stat. 2899, 2946 (2002). As used in this report, the Federal Information Security Modernization Act refers to the requirements in the 2014 law and the relevant requirements from the 2002 law that were unchanged by the 2014 law and continue in full force and effect.

[24] 15 U.S.C. § 278g-3(a) and (b).

[25] National Institute of Standards and Technology, Special Publication 800-37, Rev. 2.

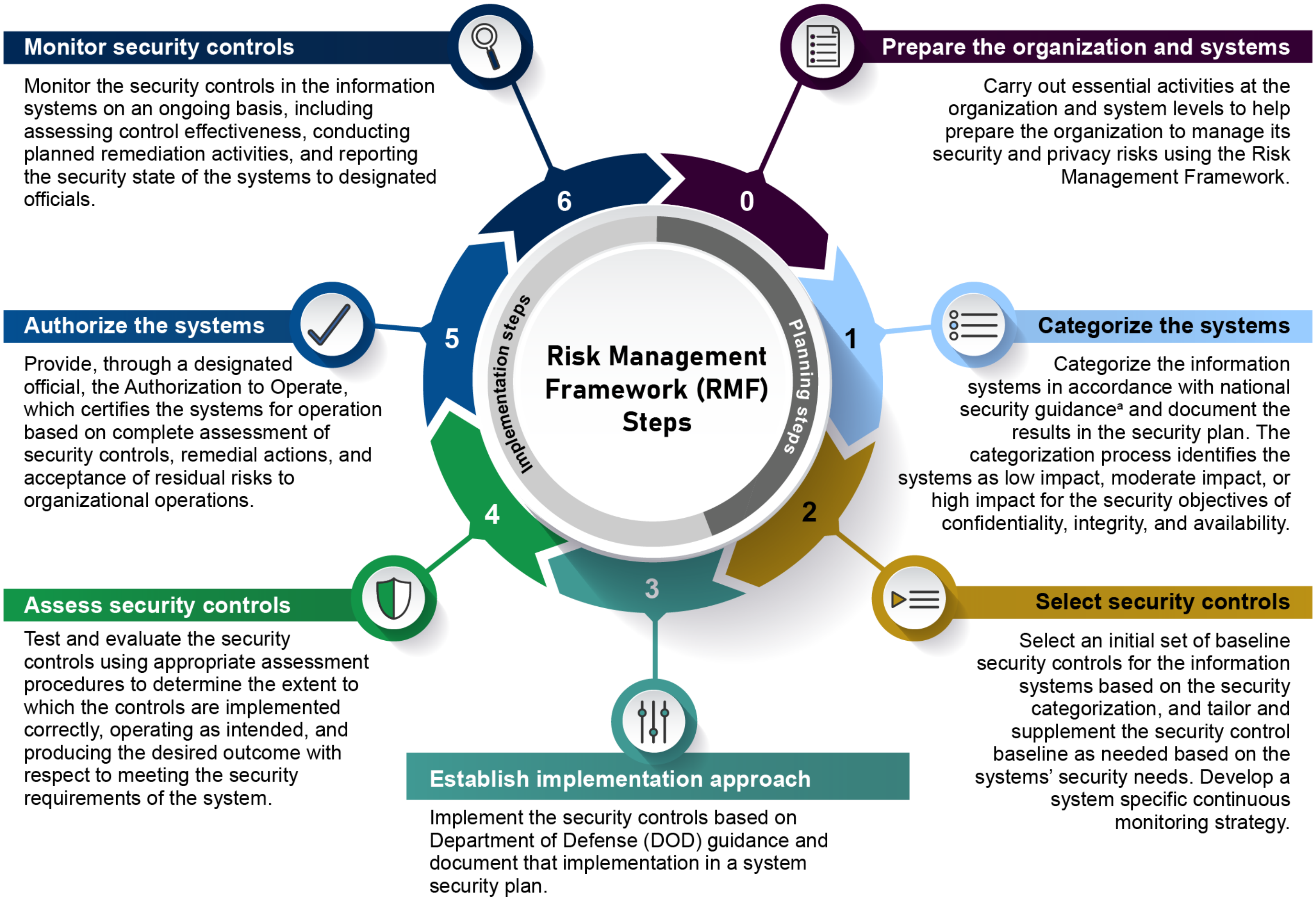
[26] National Institute of Standards and Technology, Special Publication 800-53, Rev. 5.

management framework for its IT systems.[27] This DOD instruction directs DCSA to also comply with the latest NIST guidance.

The risk management frameworks provided by NIST and DOD's CIO comprise seven steps that cover the planning, implementation, and continuous monitoring of risk management. These steps are detailed in Figure 1.

[27] Department of Defense, Office of the Chief Information Officer, DOD Instruction 8510.01.

Figure 1: Overview of DOD’s Cybersecurity Risk Management Framework Steps for IT Systems



Prepare the organization and systems

Carry out essential activities at the organization and system levels to help prepare the organization to manage its security and privacy risks using the Risk Management Framework.

Categorize the systems

Categorize the information systems in accordance with national security guidance[a] and document the results in the security plan. The categorization process identifies the systems as low impact, moderate impact, or high impact for the security objectives of confidentiality, integrity, and availability.

Select security controls

Select an initial set of baseline security controls for the information systems based on the security categorization, and tailor and supplement the security control baseline as needed based on the systems’ security needs. Develop a system specific continuous monitoring strategy.

Establish implementation approach

Implement the security controls based on Department of Defense (DOD) guidance and document that implementation in a system security plan.

Assess security controls

Test and evaluate the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the system.

Authorize the systems

Provide, through a designated official, the Authorization to Operate, which certifies the systems for operation based on complete assessment of security controls, remedial actions, and acceptance of residual risks to organizational operations.

Monitor security controls

Monitor the security controls in the information systems on an ongoing basis, including assessing control effectiveness, conducting planned remediation activities, and reporting the security state of the systems to designated officials.

Sources: GAO (icons and analysis of Department of Defense [DOD] guidance); colorlife/stock.adobe.com (illustration). | GAO-24-106179

Note: After completing the tasks in the *prepare* step, organizations executing the risk management framework for the first time for a system or set of common controls typically carry out the steps in sequential order. After organizations execute the risk management framework for the first time, the steps can be carried out in a nonsequential order.

[a] National Security Agency, Committee on National Security Systems (CNSS) Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems*, (Fort Meade, Md.: March 27, 2014).

Within this risk management framework, three steps relate to planning for cybersecurity controls:

- Step 0: Prepare the organization and systems
- Step 1: Categorize the systems

- Step 2: Select security controls

GAO's Prior Work on the Cybersecurity of Background Investigations and Sensitive Personal Information

After the 2015 OPM cybersecurity incidents, we reported in 2017 that OPM needed to improve security controls over selected high-impact systems.[28] We made five recommendations to improve security over personnel and other sensitive information, including information related to background investigations. These recommendations have been implemented.

We placed the government-wide personnel security clearance process on our High-Risk List in January 2018 due to factors that included delays in completing the security clearance process, a lack of measures to determine the quality of investigations, and issues with the IT systems supporting the process. In addition, we have designated information security as a government-wide high-risk area since 1997. Subsequently in 2003, we expanded the information security high-risk area to include the protection of critical cyber infrastructure. We further expanded this high-risk area in 2015 to include protecting the privacy of personally identifiable information. Both the government-wide personnel security clearance process and cybersecurity remain on the 2023 update to our High-Risk List.[29]

In August 2023, we reported that DOD lacked a reliable schedule for NBIS and did not have a reliable cost estimate for the program.[30] We suggested that Congress require DOD to develop a reliable schedule and cost estimate for NBIS and recommended that DOD use our survey results to improve engagement with stakeholders. As of June 2024, Congress had not taken action and DOD had not yet implemented these recommendations.

[28] GAO, *Information Security: OPM Has Improved Controls, but Further Efforts Are Needed*, GAO-17-614 (Washington, D.C.: Aug. 3, 2017).

[29] 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).

[30] GAO-23-105670.

DCSA Has Not Fully Planned for the Cybersecurity of NBIS and Legacy Systems

In its efforts to ensure the cybersecurity of NBIS and legacy systems, DCSA has not fully addressed all planning-related steps of DOD's Risk Management Framework. Specifically, DCSA

- did not fully address all required tasks in the *prepare* step,
- fully addressed all required tasks in the *categorize* step, and
- did not fully address all required tasks in the *select* step.

DCSA Did Not Fully Address Required Tasks for Preparing the Selected Systems to Manage Cybersecurity Risks

DOD's Risk Management Framework requires DCSA senior officials to prepare their organizations to execute the framework by providing context and setting priorities for privacy and security risk management.[31] The step includes 16 essential tasks that are to be carried out at either the organization or system levels. These preparatory tasks support all subsequent risk management activities.

DCSA did not fully address all the required tasks in preparation for the management of cybersecurity risks for the six selected systems. Specifically, the agency fully addressed 11 of the 16 required tasks in the *prepare* step of the risk management framework, partially addressed two tasks, and did not address three tasks. Table 1 summarizes our assessment of the extent to which DCSA addressed each task in the *prepare* step of DOD's Risk Management Framework.

Table 1: Extent to Which DCSA Policies and Practices Addressed Required Tasks in the *Prepare* Step of DOD's Risk Management Framework at the Organization and System Levels

	Required tasks in the *prepare* step	GAO assessment
Organization level	Risk management roles: identify and assign individuals key roles for executing the risk management framework.	●
	Risk management strategy: establish an organization-wide risk management strategy that includes a determination and expression of organizational risk tolerance.	●
	Risk assessment: complete an organization-wide risk assessment or update an existing risk assessment.	○
	Common control identification: identify, document, and publish common controls that are available for inheritance by organizational systems.	●
	Continuous monitoring strategy: develop and implement an organization-wide strategy for monitoring control.	●
System level	Mission or business focus: identify missions, business functions, and mission or business processes that the system is intended to support.	●

[31] Department of Defense, Office of the Chief Information Officer, DOD Instruction 8510.01.

Required tasks in the *prepare* step	GAO assessment
System stakeholders: identify the stakeholders having an interest in the system.	●
Asset identification: identify and prioritize stakeholder assets.	●
Authorization boundary: determine the authorization boundary (i.e., all components of an information system to be authorized to operate).	●
Information types: identify the types of information processed, stored, and transmitted by the system.	●
Information life cycle: identify all stages of the information life cycle for each information type the system processes, stores, or transmits.	◑
Mission-based cyber risk assessment: complete a system-level risk assessment or update an existing risk assessment.	○
Requirements definition: define and prioritize security and privacy requirements.	◑
Enterprise architecture: determine the placement of the system within the enterprise architecture.	●
Requirements allocation: allocate security and privacy requirements to the system and to the environment in which the system operates.	○
System registration: register the system for the purposes of management, accountability, coordination, and oversight.	●

● Fully addressed—the task was fully addressed for all six selected systems.

◑ Partially addressed—the task was either partially addressed for some of selected systems, or fully addressed for some systems and not addressed for others.

○ Not addressed—the task was not addressed for any of the six selected systems.

Source: GAO analysis of Defense Counterintelligence and Security Agency (DCSA) and Department of Defense (DOD) information. | GAO-24-106179

Note: DOD Instruction 8510.01 identifies two tasks as optional; therefore, they are not included as required tasks for this evaluation.

DCSA fully addressed 11 of 16 tasks in the *prepare* step. As noted in the table above, DCSA fully addressed 11 of the 16 essential tasks for preparing the organization to manage risk. For example, at the organization level, DCSA provided a list of inheritable controls and a strategy to monitor control effectiveness. At the system level, DCSA provided categorization level agreements and system security plans for each of the six selected systems. Both documents identify elements required by DOD's Risk Management Framework, including the system mission or business focus and stakeholders having an interest in the selected systems. Additionally, these documents determine the authorization boundary and identify the types of information the systems process, store, and transmit.

DCSA partially addressed two tasks in the *prepare* step. Specifically, DCSA's CIO and senior officials have either partially addressed the task related to identifying all states of the information life cycle and the task related to defining requirements or fully addressed these tasks for some selected systems but not for others.

- **Information life cycle:** DCSA did not identify all stages of the information life cycle for each information type the system processes, stores, or transmits. Specifically, four of the six systems partially addressed this task. For example, the documentation DCSA provided identified stages of the information life cycle for personally identifiable information but did not cover other identified information types, such as information security or infrastructure maintenance. The two remaining systems either did not have complete and approved documentation, or the documentation did not identify any information life cycles.
- **Requirements definition:** DCSA did not fully define and prioritize security and privacy requirements. For example, four of the six selected systems identified their privacy requirements in the privacy impact assessment. However, the two remaining privacy impact assessments were either incomplete or lacked documentation of review and approval by a senior official. Review and approval are necessary to ensure that the requirements are properly defined and aligned with the mission.

A **risk assessment** is used to identify, estimate, and prioritize risk to organizational operations, organizational assets, individuals, other organizations, and the nation, resulting from the operation and use of information systems. According to the National Institute of Standards and Technology, the purpose of risk assessments is to inform decision-makers and support risk responses by identifying relevant threats, internal and external vulnerabilities, the impact to organizations that may occur given the potential for threats exploiting vulnerabilities, and the likelihood that harm will occur. The result is a determination of risk.

Source: GAO summary of National Institute of Standards and Technology information. | GAO-24-106179

DCSA did not address three tasks in the *prepare* step. Specifically, the agency did not conduct an organization-level risk assessment, mission-based cyber risk assessment, or requirements allocation.

- **Organization-level risk assessment:** According to DCSA's CIO and system program offices, DOD conducted and documented a command cyber readiness inspection during the summer of 2023. However, the documentation provided did not address the requirements for an organization-level risk assessment. Specifically, DCSA provided an acknowledgement from the Chief of the Command Cyber Readiness Inspection Branch that DCSA had taken actions to remediate the key indicators of risk and vulnerabilities identified during the inspection. DCSA did not provide any additional documentation regarding its inspection results.
- **Mission-based cyber risk assessment:** DCSA did not provide documentation of a system-level risk assessment. The agency provided security assessment reports that included baseline information on risk by control for the selected systems. However, these reports did not include threats, the likelihood of vulnerability exploitation, or potential consequences, consistent with NIST's definition of a risk assessment report.
- **Requirements allocation:** DCSA did not provide documentation identifying how security and privacy requirements are allocated to the system and to the environment in which the system operates.

These shortfalls were allowed to occur due in part to the agency not having established an oversight process that would ensure accountability for fully completing tasks in the *prepare* step of DOD's Risk Management Framework. The Office of Management and Budget provides guidance for management to identify risks and establish internal controls to provide reasonable assurance that objectives are achieved.[32] According to DCSA officials, the agency uses standard operating procedures to manage the implementation of the framework steps. Although the standard operating procedures and DOD instructions identify tasks and who is responsible for completing them, the agency did not have an oversight process for senior officials to ensure the agency completed all tasks in the *prepare* step. Developing an oversight process will better position DCSA's CIO to fully address essential preparation activities needed to manage cybersecurity risks, such as providing context and setting priorities for privacy and security.

DCSA Fully Categorized the Security Level of Selected Systems

By **categorizing systems,** programs determine the extent to which threats could adversely impact the organization and the extent to which systems are vulnerable to these circumstances or events.

Source: GAO summary of National Institute of Standards and Technology information. | GAO-24-106179

DOD's Risk Management Framework requires programs to categorize their systems in accordance with National Security Agency (NSA) guidance.[33] The categorization process identifies each system as low impact, moderate impact, or high impact in the areas of confidentiality, integrity, and availability based on the various types of data and information the system would process, store, transmit, or protect. These categorization results are to be documented in the security plan and subsequently reviewed and approved by senior officials in the organization. In addition, security categorization results must reflect the organization's risk management strategy.

For the six selected systems, DCSA program offices fully addressed the *categorize* step of the risk management framework. Based on the information types, each DCSA program office assigned a low, moderate, or high security impact level in the areas of confidentiality, integrity, and availability. The program offices assigned these categories according to recommended levels identified by NIST and other risk factors, as required

[32] Office of Management and Budget, *Management Responsibility for Enterprise Risk Management and Internal Control*, OMB Circular No. A-123 (Washington, D.C.: July 15, 2016).

[33] National Security Agency, Committee on National Security Systems (CNSS) Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems* (Fort Meade, Md.: Mar. 27, 2014).

by NSA guidance.[34] This allowed DCSA's programs to determine the extent to which threats could adversely impact the organization and the extent to which agency systems are vulnerable to these circumstances or events.

Categorizing the system directly affects and informs other steps in the framework, from selecting security controls to defining the level of effort in assessing security control effectiveness. By categorizing its systems, DCSA took initial steps to protect the six selected systems and inform organizational risk management processes and tasks. Table 2 shows the impact levels DCSA assigned to the six selected systems.

Table 2: DCSA-Assigned Impact Levels for the Six Selected Background Investigation Systems

System	Confidentiality	Integrity	Availability	Impact
System A	High	High	Moderate	High
System B	High	High	Moderate	High
System C	High	Moderate	Moderate	High
System D	High	High	High	High
System E	High	Moderate	Moderate	High
System F	High	High	High	High

Source: GAO analysis of Defense Counterintelligence and Security Agency (DCSA) data. | GAO-24-106179

Note: We did not name the six systems in relation to the risk management steps. This information is considered controlled unclassified information and is not authorized for public release.

DCSA Selected Controls for Each System but Did Not Follow Current Guidance

According to DOD's Risk Management Framework, programs should, among other things, select controls for an IT system that are based on its security categorization and document these results.[35] The guidance states that security control baselines, descriptions, and overlays, among other things, are to be consistent with NIST Special Publication 800-53.[36] Furthermore, DOD's guidance states that during this step programs

[34] National Security Agency, Committee on National Security Systems (CNSS) Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems* (Fort Meade, Md.: Mar. 27, 2014).

[35] National Security Agency, Committee on National Security Systems (CNSS) Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems* (Fort Meade, Md.: Mar. 27, 2014).

[36] National Institute of Standards and Technology, Special Publication 800-53, Rev. 5.

should develop a continuous monitoring strategy for the system that reflects the organizational risk management strategy.

A **security control baseline** represents the minimum protection that should be provided to address the impact on an organization's confidentiality, integrity, or availability, as reflected by the system's security category.

Source: GAO analysis of National Institute of Standards and Technology information. | GAO-24-106179

Each of the DCSA program offices selected security controls for their respective IT systems based on the impact levels assigned to them in the prior step. These program offices also determined whether they needed to tailor the specific security controls to enhance the security of their systems. The selected controls and tailored actions were documented in the system security plans. Additionally, DCSA program offices developed system-level continuous monitoring strategies as called for by DOD requirements and related NIST guidance. These strategies provide information on the frequency and method for monitoring security controls and how monitoring is reported and tracked.

DCSA did not fully address all the required tasks in the *select* step of the DOD's Risk Management Framework. Specifically, DCSA selected specific security controls, but the agency did not follow current NIST security control guidance. The number of controls DCSA selected for each of the systems did not align with the latest version of NIST security control guidance (i.e., NIST Special Publication 800-53, Revision 5). NIST updated the prior guidance in September 2020. However, DCSA selected controls for each of the selected systems based on NIST Special Publication 800-53, Revision 4.

Revision 5 includes 66 new baseline security controls, 202 new control enhancements, and two new categories of controls on personally identifiable information and supply chain management.[37] Revision 5 now includes 370 baseline security controls for high impact systems and 20 control categories.

According to agency officials, DCSA uses a DOD-wide IT risk management tool to select the baseline security controls for its systems. However, officials stated that the tool is programmed to select security controls based on the outdated NIST security control guidance and not the latest version of the guidance.

DCSA officials acknowledged the variance in the selected control baselines for each of the six selected systems and stated that DOD has not yet implemented the current NIST guidance across the department. As a result, DOD's IT risk management tool does not allow for the

[37] National Institute of Standards and Technology, Special Publication 800-53, Rev. 5.

selection of security controls identified in the updated NIST guidance. Moreover, DCSA has not implemented any additional security controls to compensate for the risk management tool's lack of updated controls. DCSA officials stated that this is because DOD's CIO has not instructed DCSA to do so. DOD issued a memo in October 2023 announcing the department's adoption and transition timeline to Revision 5. Subsequently, in November 2023, DOD issued a notice that the Revision 5 updates had been activated in the department's IT risk management tool.

However, DCSA was not included as one of the organizations granted access to the updated tool. Until DOD's CIO revises policies, procedures, and the process for selecting baseline security controls to be consistent with current NIST guidance and grants DCSA access to the updated tool, DCSA cannot be assured the agency will have the minimum protection necessary to effectively manage security risks.

DCSA Did Not Fully Implement Privacy Controls for Selected Background Investigation Systems

NIST SP 800-53 provides guidance on privacy controls to protect organizational operations and assets, individuals, other organizations, and the nation from a diverse set of threats and risks. These include hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. Further, SP 800-53 is periodically revised to incorporate new technologies and address changing threats, with the most recent (revision 5) published in 2020.

Table 3 identifies the four control areas and eight selected privacy controls we assessed for NBIS and legacy systems.

Table 3: Control Areas and Privacy Controls for Selected Background Investigation Systems

Areas	Control
Developing policies and procedures	Access control policy and procedures
	Awareness and training policy and procedures
	System and information integrity policy and procedures
Delivering training	Security awareness training
	Role-based training
Defining and reviewing types of events to log	Event logging
Assessing selected controls and system risks	Control assessment
	Risk assessment

Source: GAO analysis of Defense Counterintelligence and Security Agency data. | GAO-24-106179

DCSA's progress on implementing the control areas and controls was mixed.

- **Developing policies and procedures:** DCSA's CIO has developed policies and procedures to address the selected privacy controls but did not document key information or have evidence of review or updates.
- **Delivering training:** All sampled users of the selected systems have completed security training; however, DCSA has not ensured all training and certifications are current.
- **Defining and reviewing types of events to log:** DCSA has defined types of events to be logged and described how long logs are to be retained to support investigations. However, the agency has not provided a rationale for why the selected event types can support incident investigations or defined a frequency for reviewing and updating which types of events are to be logged.
- **Assessing selected controls and system risks:** DCSA program offices assessed security controls for the six selected systems but did not use an assessment plan as a guide. Further, DCSA has not conducted risk assessments for the six selected systems.

DCSA's Policies and Procedures for Selected Privacy Controls Did Not Document Key Information or Have Evidence of Review

NIST recommends that organizations develop policies and procedures that address the privacy controls. NIST groups privacy controls into 20 categories that align with minimum security requirements. Each control category contributes to the agency's security and privacy assurance. According to NIST, policies should address the purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities in a manner consistent with laws and guidance. Procedures should facilitate the implementation of the applicable policy and the associated controls within the control family, describe how the policies or controls are implemented, and be documented in a system security or privacy plan.[38] NIST also recommends that agencies periodically review and update policies and procedures based on assessment or audit findings, security incidents or breaches, or changes in laws and guidance.[39]

DCSA's CIO has developed policies and procedures to address the selected privacy controls but did not document key information or have

[38] National Institute of Standards and Technology, Special Publication 800-53, Rev. 5.

[39] National Institute of Standards and Technology, Special Publication 800-53, Rev. 5.

evidence of review or updates. Specifically, the CIO has developed policies and procedures to guide the agency's implementation of the control families for access, awareness and training, and system and information integrity, as well as the associated controls. The agency also relies on DOD directives and manuals as policies for all controls. DCSA officials noted agency-specific policies are preferable to relying solely on DOD policies. DCSA program officials also told us they develop procedural documents at the program level to satisfy a security control as needed.

However, DCSA's policies and procedures for selected privacy controls did not consistently document key information. Specifically, they did not include information such as scope or descriptions for implementation as required by NIST. For instance, DCSA provided a DOD policy on training instead of an agency security awareness training policy. This policy did not contain requirements for security and privacy training or information about the content of training. DCSA's access control policy required awareness training for normal and privileged users but did not contain procedures for implementation. Though DCSA has established policies, they lack required details, which can impede the agency's efforts to comply with the NIST requirements.

Moreover, DCSA has not continuously reviewed or updated its policies and procedures as required by NIST. Specifically, DCSA's policy and procedure documentation did not define a time frame for reviewing and updating the guidance. As a result, this control requirement had not been consistently implemented. For example, the NBIS Access Control Plan requires quarterly review, but there is no evidence this plan has been reviewed.

According to DCSA CIO officials, agency policies are living documents that are reviewed on a yearly basis and updated as necessary. *Standards for Internal Control in the Federal Government* requires agency management to review policies to ensure continued effectiveness in achieving the agency's objectives.[40] While having an informal practice for reviewing and updating policies and procedures demonstrates an effort to implement this internal control requirement, the lack of consistency in the

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

updates underscores the oversight challenges that remain for ensuring the tasks are completed.

DCSA Did Not Ensure Users Had Current Training and Certifications

NIST recommends that organizations provide security and privacy literacy training to system users and include measures to test the knowledge of the users. According to NIST, the training content should include an understanding of the need for security and privacy as well as actions by users to maintain security and personal privacy and to respond to suspected incidents. The content should address the handling of personally identifiable information, among other things.

NIST also recommends role-based training for users with management, operational, and technical roles and responsibilities covering physical, personnel, and technical controls. Role-based training also includes policies, procedures, tools, methods, and artifacts for the security and privacy roles defined.

Additionally, DCSA's access control policy requires all system users to complete DOD's cyber awareness training before account access is granted and maintain it annually. Further, DCSA's policy requires privileged users to undergo additional training for certifications.

All sampled users of the selected systems had completed security training; however, DCSA did not ensure all training and certifications were current. Specifically, as of September 2023, most sampled users with direct access to NBIS systems (86 percent) had received DOD security awareness training as required, but 14 percent of users had out-of-date training.[41] However, by December 2023, DCSA was able to provide evidence of current training for all but one person. According to DCSA officials, system users, including privileged users, complete self-paced, web-based training through a DOD portal. DCSA officials also stated they use alternative training techniques to expand security awareness literacy, such as posters, computer pop-ups, and emails.

Additionally, almost all privileged users had required certifications, but not all certifications were up to date. Specifically, out of the 64 personnel sampled, 19 had privileged access to NBIS systems, and all but one of them had certifications to meet the privileged user training requirement.

[41] The margin of error for the estimate is +/- 8.6% with 95% confidence. See appendix 1 for more detailed methodology.

However, as of December 2023, four of the privileged users had certifications that were expired.

DCSA Has Not Fully Defined the Types of Events to be Logged

NIST requires organizations to support audit and monitoring capabilities by logging certain events that occur on organizational systems. NIST further recommends providing a rationale that explains why the event types selected for logging are adequate to support investigating incidents that may occur. According to NIST, events that are significant and relevant to the security of systems and the privacy of individuals should be logged. Recognizing that the types of events that organizations need to log may change, NIST recommends reviewing and updating the types of logged events to help ensure that the events remain relevant and continue to support the needs of the organization.

DCSA has defined types of events to be logged and described how long logs are to be retained to support investigations but has not provided a selection rationale or a frequency for reviewing and updating which types of events are to be logged. Specifically, the agency defined how often event logs are to be reviewed, specified the tools used for analysis, and described the procedures to manage any suspected incidents. Additionally, DCSA has provided evidence that at least some potential incidents identified by log analysis have been further investigated.

However, DCSA has not provided a rationale to explain why the selected types of events logged are adequate to support after-the-fact investigations. According to DCSA officials, DCSA inherited the rationale for the selection of event types from DOD. However, DCSA could not provide documentation of the rationale behind the types of events to be logged. Although DCSA relies on DOD requirements to guide their selection of controls, it has not ensured there is a rationale for why the selected events would adequately support an investigation. Without a defined rationale for selecting the types of events to be logged, it is possible that DCSA is wasting resources logging superfluous events or increasing its risk by not logging all pertinent events.

Moreover, DCSA has not defined a frequency for reviewing and updating which types of events are to be logged. According to DCSA, the agency is automatically compliant with this control because they are covered at the DOD level. Specifically, the control implementation guidance states that DOD defines the frequency of auditing for each type of event to be logged. However, DCSA's own policies require an annual review, for which there is no evidence. Without a periodic review of event types to be logged, the agency cannot be sure that they are logging all events necessary to support the investigation of incidents.

DCSA Did Not Develop an Assessment Plan or Conduct Risk Assessments for Selected Systems

NIST requires organizations to conduct control assessments and risk assessments. Specifically, organizations should identify a qualified assessor, develop a control assessment plan that describes the scope of the assessment, have the plan reviewed and approved by a designated senior officer, and assess the controls in the system and its environment. According to NIST, the assessment results should be documented in a report that provides details on the accuracy and completeness of the reports and whether the controls are implemented correctly, operating as intended, and producing the desired outcomes. NIST states that report results should be provided to designated senior officials with roles relevant to the assessment type.

A **control assessment** tests or evaluates the controls in an information system or an organization to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security or privacy requirements for the system or the organization.

A **risk assessment** is the process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the nation, resulting from the operation of a system.

Source: GAO summary of National Institute of Standards and Technology information. | GAO-24-106179

In addition, NIST guidance recommends that organizations conduct a risk assessment that identifies threats and vulnerabilities and determines their likelihood and impact to systems and the information it processes, stores, or transmits. NIST also recommends that organizations assess potential risks to individuals as a result of personal information processed by the system. The results of the risk assessments should be documented, reviewed, and disseminated.

DCSA program offices assessed security controls for the six selected systems but did not use an assessment plan as a guide or conduct risk assessments for the six selected systems. DCSA program offices for the six selected systems assessed the implementation of the selected security controls to determine whether they were implemented in compliance with defined requirements. For example, DCSA provided security assessment reports for each selected system that outlines which controls are compliant and noncompliant with NIST guidance.

However, the designated authorizing officials for the six selected systems did not review and approve control assessment plans before the assessments were conducted. Additionally, the agency did not document the objectives for the six selected systems’ control assessments or detail how to conduct such assessments in a manner consistent with NIST’s definition of an assessment plan. According to DCSA officials, the security plan for each system serves as its control assessment plan. While a system security plan provides an overview of the security requirements for an information system and describes the security controls in place for meeting those requirements, it does not fully address NIST guidance. For example, it does not describe the scope of the assessment or identify threats and vulnerabilities to the systems and data. Without assessment plans, DCSA's authorizing official could be unable to establish the appropriate expectations for the control assessment, determine the level of effort needed, and ensure that an appropriate number of resources are applied to determine security control effectiveness.

Additionally, DCSA officials told us that the agency has assessed risk for the six selected systems and the resulting risk assessment report is in each system's authorization package. However, the authorization packages we reviewed did not include a risk assessment report or the formal output from the process of assessing risk, consistent with NIST's definition of a risk assessment report. The authorization packages included security assessment reports for each of the selected systems. These reports provide baseline information on risk by control; however, they do not provide a holistic view of threats and resulting risks that can exist independent of control implementation. A risk assessment that documents a holistic view of threats could help inform DCSA senior officials and support risk responses by identifying relevant threats, vulnerabilities, and impact to the organization as well as the likelihood that harm will occur. In addition, a risk assessment could help address the impact on individuals in the event of a breach similar to the 2015 OPM incidents previously discussed.

Privacy Control Shortfalls Were Largely Allowed to Occur Due to the Lack of a Process to Ensure CIO Oversight

According to DCSA's *Annual Review Standard Operating Procedure*, system program officials are to evaluate all NIST controls annually, verify that each control is implemented correctly and completely, and mark the control as compliant, noncompliant, or not applicable in DOD risk management. Additionally, *Standards for Internal Control in the Federal Government* highlights the need for an oversight body to oversee management's design, implementation, and operation of the entity's organizational structure so that the processes necessary to enable the oversight body to fulfill its responsibilities exist and are operating effectively.[42]

Many of the shortfalls identified in this report were allowed to occur due to the lack of an oversight process to ensure DCSA's CIO verifies that controls marked as compliant have been properly assessed. For example, of the eight controls associated with each of the six selected systems (i.e., 48 control instances), DCSA senior program officials

[42] GAO-14-704G.

marked 40 as being compliant with NIST guidance. These controls were reviewed by the security control assessor and ultimately approved by an authorizing official. However, the controls marked as compliant had requirements that had not been fully implemented, as previously discussed.

According to DCSA officials, the agency uses corrective action plans to monitor the remediation of noncompliant controls. DCSA has developed corrective action plans for the eight controls marked noncompliant, and DCSA's Chief Information Officer monitors corrective actions for noncompliant controls on a monthly basis. While monitoring corrective actions may help DCSA officials oversee how identified shortfalls are being addressed, this step does not provide DCSA's CIO the visibility needed to ensure that all deficient controls have been identified. Although DCSA officials followed their annual review workflow to review and approve assessed controls, the agency's corrective action plans do not have an oversight process to ensure control determinations were properly assessed and appropriately marked.

Until DCSA establishes an oversight process for confirming that control requirements have been accurately completed prior to implementation, the agency may be hindered in identifying and remediating shortfalls in privacy controls. This increases the risk that sensitive information contained in or processed by NBIS and legacy systems could be disclosed, altered, or used inappropriately.

Conclusions

As the federal government's primary service provider for background investigations, DCSA is tasked with ensuring the NBIS and legacy systems used in these investigations are properly secured from breaches similar to the 2015 OPM incidents that compromised federal security clearance files. While DCSA has taken steps to prepare for managing security risks to NBIS and legacy systems, the agency has not fully addressed key tasks in DOD's Risk Management Framework, largely due to a lack of an oversight process. These key tasks include identifying all stages of the information life cycle, defining and prioritizing security and privacy requirements, performing risk assessments at both the organizational and system levels, and allocating security and privacy requirements to the appropriate systems. Until DCSA's CIO establishes an oversight process to ensure the tasks in DOD's Risk Management Framework's *prepare* step are fully addressed, the agency's leadership will be less able to identify, prioritize, and mitigate privacy and security risks, and important background investigation systems could be underprotected.

Moreover, since the DOD-wide IT risk management tool had not been updated to correspond with current NIST guidance, the agency's selection of security control baselines did not include all required controls.[43] Until DOD revises its process for selecting baseline security controls to be consistent with current NIST guidance and grants DCSA access to the updated tool, DCSA's CIO will be unable to ensure the security control baselines that the agency selects include these additional controls. Consequently, the agency will not be able to assess the impact risks could have on the confidentiality, integrity, or availability of data in its systems.

DCSA partially implemented the eight selected privacy controls related to developing policies and procedures, delivering training, establishing event logging requirements, and assessing selected controls and system risks for the selected systems. This is due, in part, to DCSA's CIO not establishing an oversight process for these privacy controls. Until the agency fully implements all privacy controls as required and establishes an oversight process to ensure implementation, it risks the inadvertent or malicious disclosure, alteration, or loss of sensitive information in its NBIS and legacy systems.

Recommendations for Executive Action

We are making the following 13 recommendations to the Secretary of Defense.

The Secretary of Defense, in coordination with the DCSA Director, should ensure DCSA's Chief Information Officer identifies and documents all stages of the information life cycle for each information type the system processes, stores, or transmits. (Recommendation 1)

The Secretary of Defense, in coordination with the DCSA Director, should ensure DCSA's Chief Information Officer fully defines, prioritizes, and documents security and privacy requirements. (Recommendation 2)

The Secretary of Defense, in coordination with the DCSA Director, should ensure DCSA's Chief Information Officer completes an organization-wide risk assessment and documents the results. (Recommendation 3)

[43] DOD Instruction 8510.01 directs DCSA to also comply with the latest NIST guidance.

The Secretary of Defense, in coordination with the DCSA Director, should ensure DCSA's Chief Information Officer completes system-level risk assessments and documents the results. (Recommendation 4)

The Secretary of Defense, in coordination with the DCSA Director, should ensure DCSA's Chief Information Officer allocates security and privacy requirements to the system and to the environment in which the system operates and documents the results. (Recommendation 5)

The Secretary of Defense, in coordination with the DCSA Director, should ensure DCSA's Chief Information Officer establishes an oversight process to ensure senior officials complete all tasks in the risk management framework's *prepare* step. (Recommendation 6)

The Secretary of Defense, in coordination with the DCSA Director, should ensure DCSA's Chief Information Officer updates the selected security control baselines for NBIS and legacy systems to correspond with the current version of NIST Special Publication 800-53 after DOD updates the relevant guidance. (Recommendation 7)

The Secretary of Defense should ensure DOD's Chief Information Officer updates the department's policies and procedures related to the Risk Management Framework to use the current version of NIST Special Publication 800-53. (Recommendation 8)

The Secretary of Defense should direct DCSA's Chief Information Officer to ensure the agency's policies and procedures include key information and are reviewed and updated as required. (Recommendation 9)

The Secretary of Defense should direct DCSA's Chief Information Officer to ensure all security training and certifications for its system users are current. (Recommendation 10)

The Secretary of Defense should direct DCSA's Chief Information Officer to ensure the agency establishes a rationale for why the selected event types can support incident investigations and defines a frequency for reviewing and updating which types of events are to be logged. (Recommendation 11)

The Secretary of Defense, in coordination with the DCSA Director, should ensure that control assessment plans are documented and that assessments align with these plans. (Recommendation 12)

The Secretary of Defense, in coordination with the DCSA Director, should ensure DCSA's Chief Information Officer establishes an oversight process to ensure senior DCSA officials fully implement the recommended tasks for the required privacy controls. (Recommendation 13)

Agency Comments and Our Evaluation

We provided a draft of this report to DOD for their review and comment. In its written comments, DOD stated that it concurred with comment on 12 of the 13 recommendations and non-concurred with the remaining one.

For the 12 recommendations with which it concurred, DOD described actions it has taken and plans to take to address them. For example, with respect to recommendations aimed at addressing tasks that prepare for the management of cybersecurity risks (Recommendations 1 through 6), DOD plans to:

- Audit documentation of NBIS and legacy systems external inventory, application services, and privacy impact assessments by August 2024. (Recommendations 1 and 2)
- Integrate NBIS/legacy systems into its existing oversight processes, including execution of the Cybersecurity Product Evaluations (CPE) process to perform initial risk assessments no later than October 2024. (Recommendation 4)
- Conduct a comprehensive review of NBIS/legacy systems control postures no later than July 2024. (Recommendation 5)
- Address the remaining five tasks no later than March 2025. (Recommendation 6)

Regarding recommendation 3, DOD stated it will consolidate documentation supporting the organization-wide risk assessment tasks into one product consistent with NIST Cybersecurity Framework and DODI 8510.01 guidance. DOD stated this updated product will include risk assessment reviews, the Cybersecurity Risk Management Strategy, and command cyber readiness inspection results. Additionally, DOD stated it had provided us all documentation related to its command cyber readiness inspection results and recommended we clarify this in the report.

As previously mentioned in this report, DCSA's documentation related to its command cyber readiness inspection results did not address the requirements for an organization-level risk assessment. Specifically, DCSA provided an acknowledgement from the Chief of the Command

Cyber Readiness Inspection Branch that DCSA had taken actions to remediate key indicators of risk and vulnerabilities identified during the inspection. DCSA did not provide any additional documentation regarding its inspection results.

DOD agreed with our recommendation to update the selected security control baselines for NBIS and legacy systems to correspond with the current version of NIST Special Publication 800-53 (Recommendation 7). In its written comments, DOD reiterated its plan to conduct a comprehensive review of NBIS/legacy systems control postures no later than July 2024.

With respect to our recommendations aimed at implementing tasks for the required privacy controls (recommendations 9 through 13), DOD described plans to update its policies and procedures by October 2024 (recommendation 9); revalidate training compliance for all system users by June 2024 (recommendation 10); implement DCSA's Security Operations Center Integration Strategy in phases ending in September 2024 (recommendation 11); and consolidate existing NBIS/legacy systems documentation into a formal Security Assessment Plan by September 2024 (recommendation 12). In addition, DOD reiterated its plan to integrate NBIS/legacy systems into existing oversight processes (recommendation 13). Further, DOD described plans to update appointment orders for information system owners, program managers, and other key personnel in NBIS/legacy systems by June 2024.

DOD disagreed with recommendation 8. This recommendation calls for DOD's CIO to update the department's policies and procedures related to the Risk Management Framework to use the current version of NIST Special Publication 800-53. In its written comments, DOD stated that the DOD CIO did not participate in this review and recommended the deletion of this recommendation. Additionally, DOD stated it has included guidance in DODI 8510.01 and issued a memo in October 2023 regarding the department's adoption and transition timeline to NIST Special Publication 800-53 Revision 5, which includes clarifying instructions on implementation of additional security controls.

However, we believe the recommendation is warranted. We met with the DOD CIO's office in May 2023 to discuss how DOD-level cybersecurity policies were applicable to NBIS and legacy systems. In that meeting, the DOD CIO official told us that the department was discussing its transition to Revision 5 and would be creating a migration timeline. As previously mentioned in this report, DOD issued a memo in October 2023 announcing the department’s adoption and transition timeline to Revision 5. According to the memo, systems that have a current authorization decision should develop a strategy and schedule for the transition that must not exceed the system re-authorization timeline of every three years. The six background investigation systems we selected each received approval or authorization to operate on the DOD network between July 2023 and November 2023. Thus, these six systems will need to establish strategies and schedules within three years of their authorization dates. DOD needs to provide documentation of DCSA’s strategy and schedule for implementing these additional controls. We will follow up to confirm that the department’s actions on this recommendation are, to the extent possible, achieving the desired results. If confirmed, we will take steps to close the recommendation.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Defense, and other interested parties. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you have any questions about this report, please contact Jennifer R. Franks at (404) 679-1831 or FranksJ@gao.gov or Alissa H. Czyz 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. GAO staff who made key contributions to this report are listed in appendix III.

Jennifer R. Franks
Director, Center for Enhanced Cybersecurity
Information Technology and Cybersecurity

Alissa H. Czyz

Alissa H. Czyz
Director, Defense Capabilities and Management

Appendix I: Objectives, Scope, and Methodology

The objectives of our review were to determine the extent to which the Defense Counterintelligence and Security Agency (DCSA) (1) planned for cybersecurity controls for the National Background Investigation Services (NBIS) system and legacy background investigation systems and (2) implemented privacy controls for these systems. This report builds on work in our August 2023 NBIS report.[1]

To select the NBIS and legacy systems for review, we asked DCSA to provide us with an inventory of their background investigation systems. The inventory revealed that DCSA had seven NBIS systems and 11 legacy systems. We narrowed down our review selection based on the system's role in data processing. Specifically, we chose the roles of data repository, user interaction, administrative interaction, data processing, and transmission because these are critical to the data processing operations (i.e., data flow in transit and at rest) of the NBIS system.

For our review, we selected three NBIS systems and three legacy systems described in Table 4 below.

Table 4: Selected NBIS and Legacy Background Investigation Systems

Program	System	System description
National Background Investigation Services (NBIS) systems	Data management subsystem	Provides data logistics that support the federal background investigations systems. This subsystem expedites information sharing and reduces processing times for acquiring NBIS Investigative Management system data.
	Development, security, and operations	Performs cybersecurity correlation and analysis of log files. It also generates resultant dashboard information on security posture and supports cybersecurity monitoring and cybersecurity scanning of hosts. Additionally, this system supports the development of applications subsystems that comprise the NBIS system.
	Electronic application	Provides a web-based interface for information that investigators need to begin a federal background investigation to determine suitability for a security clearance. This system will replace the legacy Electronic Questionnaires for Investigations Processing system.
Legacy background investigation systems	Electronic Questionnaires for Investigations Processing	Provides a web-based interface that facilitates the processing of standard investigative forms used during background investigations.
	Personnel Investigation Processing System	Maintains DCSA's Security and Suitability Investigations Index and provides a broad range of support for the background investigation process, including receiving security information, scheduling, transmitting investigation requests, closing investigations, transmitting results, and tracking all stages.

[1] See 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).

Program	System	System description
	Office of Personnel Management Personnel Investigation Processing Imaging System	Provides a range of imaging services, such as paper-to-electronic-document conversion, quality assurance, as well as image storage, retrieval, and release.

Source: GAO analysis of Defense Counterintelligence and Security Agency (DCSA) information. | GAO-24-106179

To determine the extent to which DCSA planned for cybersecurity controls for the NBIS system and legacy background investigation systems, we reviewed Department of Defense (DOD) and DCSA cybersecurity guidance and documents related to risk management. For example, we reviewed documents DCSA officials use to implement, oversee, and demonstrate compliance with risk management steps, such as policies and procedures at the organizational level and practices at the system level. Specifically, we reviewed the system categorization results, system security plans, security assessment reports, privacy impact assessments, continuous monitoring strategy, as well as documentation on the common control provider and authorizations to operate, where available. We evaluated these documents and data against required tasks from the first three risk management steps identified in DOD's Risk Management Framework.[2] For the purpose of this review, we focused on the first three steps, which address planning for cybersecurity risk management—*prepare* the system, *categorize* the system, and *select* security controls.

In addition to evaluating DCSA's efforts against guidance in DOD's instruction on cybersecurity risk management, we also evaluated these efforts against the *prepare, categorize*, and *select* steps in the National Institute of Standards and Technology's (NIST) risk management framework[3] and the *categorize* and *select* steps in the Committee on National Security Systems Instruction No. 1253,[4] because DOD's *Risk*

[2] Department of Defense, Office of the Chief Information Officer, *DOD Risk Management Framework (RMF) for Information Technology (IT) Systems*, DOD Instruction 8510.01 (July 19, 2022). This framework identifies seven key risk management steps (each of which includes several tasks that must be performed).

[3] National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations*, NIST Special Publication 800-37, Revision 2 (Dec. 2018).

[4] National Security Agency, Committee on National Security Systems, *Security Categorization and Control Selection for National Security Systems*, Instruction No. 1253 (July 2022).

Management Framework for DOD Systems instruction directs DCSA to also comply with these documents.[5]

We supplemented our analysis of documents and data by interviewing officials in DOD's and DCSA's Office of the Chief Information Officer and the system program offices about their efforts to implement, assess, document, and review risk management tasks for their respective systems. We then made determinations based on the documents and data provided about the extent to which each system's program office had fully addressed, partially addressed, or not addressed the required tasks for the risk management step.

- Fully addressed – when the documentation provided by DCSA addressed all tasks in the risk management step, we determined that DCSA "fully addressed" the step.
- Partially addressed – when the documentation, addressed some but not all tasks in the risk management step for some of the selected the systems or fully addressed the tasks for some systems and not addressed for others, we determined that DCSA "partially addressed" the step.
- Not addressed – when the documentation did not address any part of the risk management step, we determined the step was "not addressed."

To assess the implementation of privacy controls for the selected NBIS and legacy systems, we reviewed NIST Special Publication 800-53 Revision 5 to identify the baseline controls for protecting an individual's privacy.[6] Because there are 96 baseline controls for privacy, we narrowed down our selection by mapping these controls to critical elements in our *Federal Information System Controls Audit Manual* critical elements,[7] and

[5] Department of Defense, Office of the Chief Information Officer, DOD Instruction 8510.01.

[6] National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, NIST Special Publication 800-53, Rev. 5 (Sept. 2020). NIST Revision 5 identifies security and privacy controls that organizations can use to protect their systems.

[7] GAO, *Federal Information System Controls Audit Manual*, GAO-09-232g (Washington, D.C.: Feb. 9, 2009). This manual contains guidance for reviewing information system controls that affect the confidentiality, integrity, and availability of computerized information. The manual's critical elements are tasks that are essential for establishing adequate information system controls.

our *Cybersecurity Program Audit Guide* primary components.[8] Based on this analysis, we selected eight privacy controls for review, described in the table below.

Table 5: Summary of Selected Privacy Controls for National Background Investigation Services and Legacy Background Investigation Systems

Category	Control
Delivering training	AT-2 Security awareness training
	AT-3 Role-based training
Developing policies and procedures	AC-1 Access control policy and procedures
	AT-1 Awareness and training policy and procedures
	SI-1 System and information integrity policy and procedures
Establishing event logging procedures	AU-2 Event logging
Assessing selected controls and system risks	CA-2 Control assessment
	RA-3 Risk assessment

Source: GAO summary of National Institute of Science and Technology information. | GAO-24-106179

We analyzed documents used by DCSA officials to implement, oversee, and demonstrate compliance with the eight selected controls for each of the six systems. We evaluated system privacy documentation and data against NIST guidance for the eight selected controls.

To estimate the percentage of DCSA personnel that received security training, we analyzed training data from a random sample of personnel with direct access to NBIS systems. DCSA provided a list of these personnel, and we selected a random sample of 72 personnel from the population of 287. We reviewed security training certificates for the 64 personnel who remained at the agency when we received the data to determine an estimate of the percentage of personnel in the population that had up-to-date security training. Additionally, we identified the personnel in our sample with privileged access to NBIS systems to determine how many of them had received required privileged user training. Because the sample was not made based on privileged access, the privileged user training result is nongeneralizable.

[8] GAO, *Cybersecurity Program Audit Guide*, GAO-23-104705 (Washington, D.C.: Sept. 2023). This guide contains guidance for conducting cybersecurity performance audits.

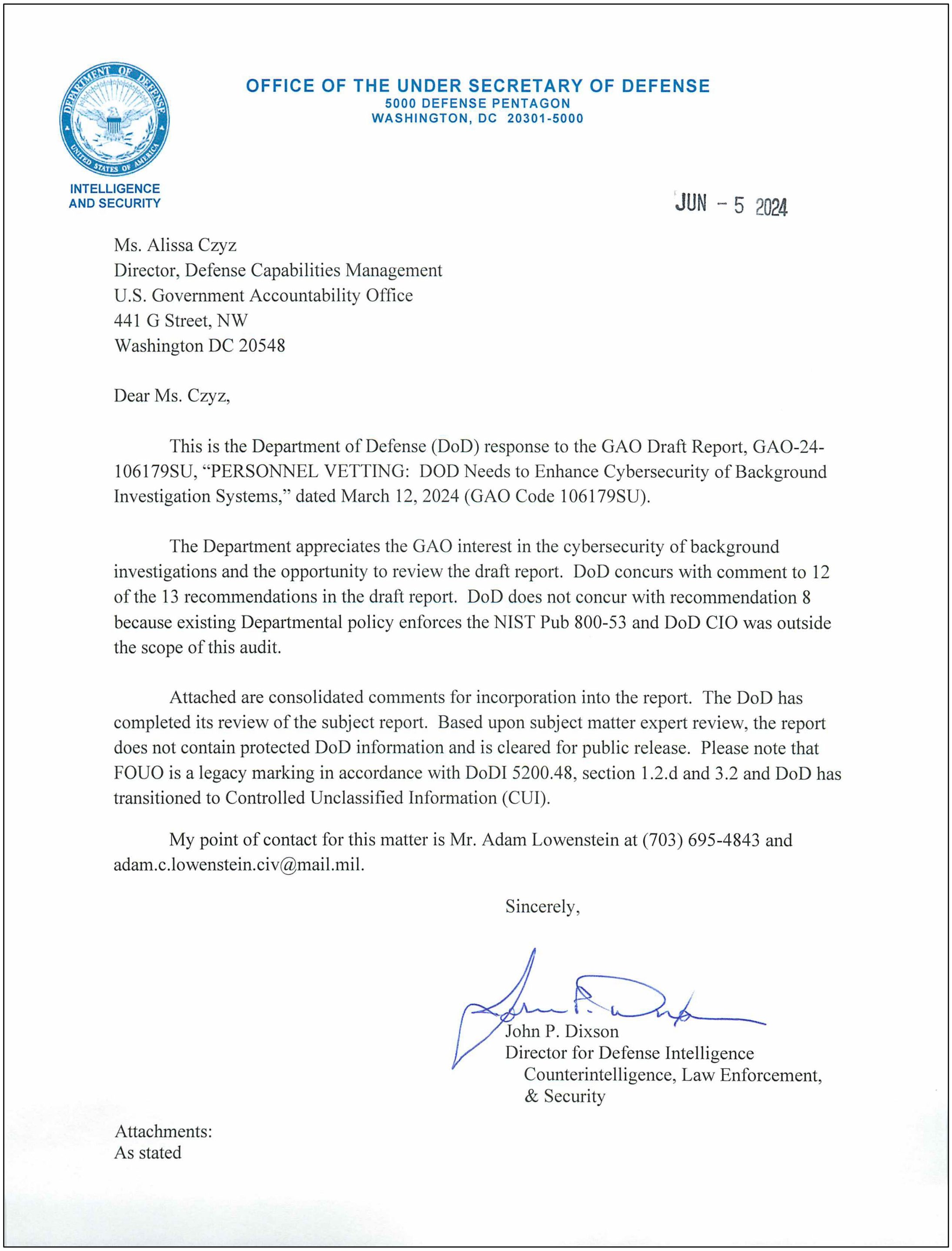
We supplemented our analysis of documents and data by interviewing officials in DCSA's Office of the Chief Information Officer and the system program offices about their efforts to implement, assess, document, and review selected privacy control tasks for their respective systems. We then used professional judgment to determine the extent to which each system's program office had fully addressed, partially addressed, or not addressed all controls.

- Fully addressed – when the documentation provided by DCSA addressed all requirements, we determined that DCSA "fully addressed" the control.
- Partially addressed – when the documentation addressed some but not all requirements for the selected systems or fully addressed for some systems and not addressed for others, we determined that DCSA "partially addressed" the control.
- Not addressed – when the documentation did not address any part of the control requirement, we determined the control was "not addressed."

Additionally, we have ongoing work assessing DCSA's implementation of cybersecurity controls for the NBIS system, which we will publish in a subsequent report with limited distribution due to the sensitivity of the material covered.

We conducted this performance audit from August 2022 to June 2024 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.

Appendix II: Comments from the Department of Defense



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

INTELLIGENCE
AND SECURITY

JUN - 5 2024

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

Dear Ms. Czyz,

This is the Department of Defense (DoD) response to the GAO Draft Report, GAO-24-106179SU, "PERSONNEL VETTING: DOD Needs to Enhance Cybersecurity of Background Investigation Systems," dated March 12, 2024 (GAO Code 106179SU).

The Department appreciates the GAO interest in the cybersecurity of background investigations and the opportunity to review the draft report. DoD concurs with comment to 12 of the 13 recommendations in the draft report. DoD does not concur with recommendation 8 because existing Departmental policy enforces the NIST Pub 800-53 and DoD CIO was outside the scope of this audit.

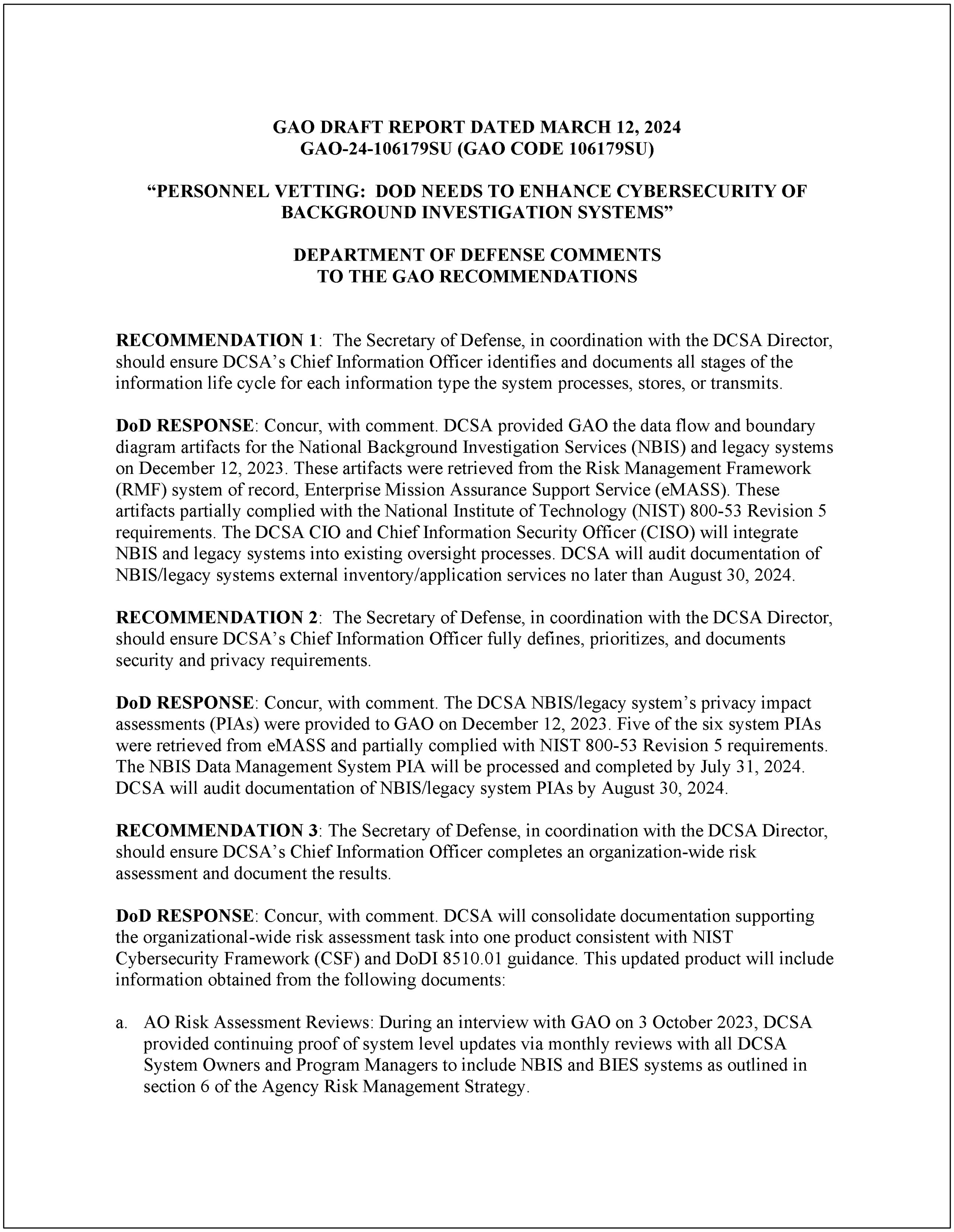
Attached are consolidated comments for incorporation into the report. The DoD has completed its review of the subject report. Based upon subject matter expert review, the report does not contain protected DoD information and is cleared for public release. Please note that FOUO is a legacy marking in accordance with DoDI 5200.48, section 1.2.d and 3.2 and DoD has transitioned to Controlled Unclassified Information (CUI).

My point of contact for this matter is Mr. Adam Lowenstein at (703) 695-4843 and adam.c.lowenstein.civ@mail.mil.

Sincerely,

John P. Dixson
Director for Defense Intelligence
Counterintelligence, Law Enforcement,
& Security

Attachments:
As stated



GAO DRAFT REPORT DATED MARCH 12, 2024
GAO-24-106179SU (GAO CODE 106179SU)

"PERSONNEL VETTING: DOD NEEDS TO ENHANCE CYBERSECURITY OF BACKGROUND INVESTIGATION SYSTEMS"

DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATIONS

RECOMMENDATION 1: The Secretary of Defense, in coordination with the DCSA Director, should ensure DCSA's Chief Information Officer identifies and documents all stages of the information life cycle for each information type the system processes, stores, or transmits.

DoD RESPONSE: Concur, with comment. DCSA provided GAO the data flow and boundary diagram artifacts for the National Background Investigation Services (NBIS) and legacy systems on December 12, 2023. These artifacts were retrieved from the Risk Management Framework (RMF) system of record, Enterprise Mission Assurance Support Service (eMASS). These artifacts partially complied with the National Institute of Technology (NIST) 800-53 Revision 5 requirements. The DCSA CIO and Chief Information Security Officer (CISO) will integrate NBIS and legacy systems into existing oversight processes. DCSA will audit documentation of NBIS/legacy systems external inventory/application services no later than August 30, 2024.

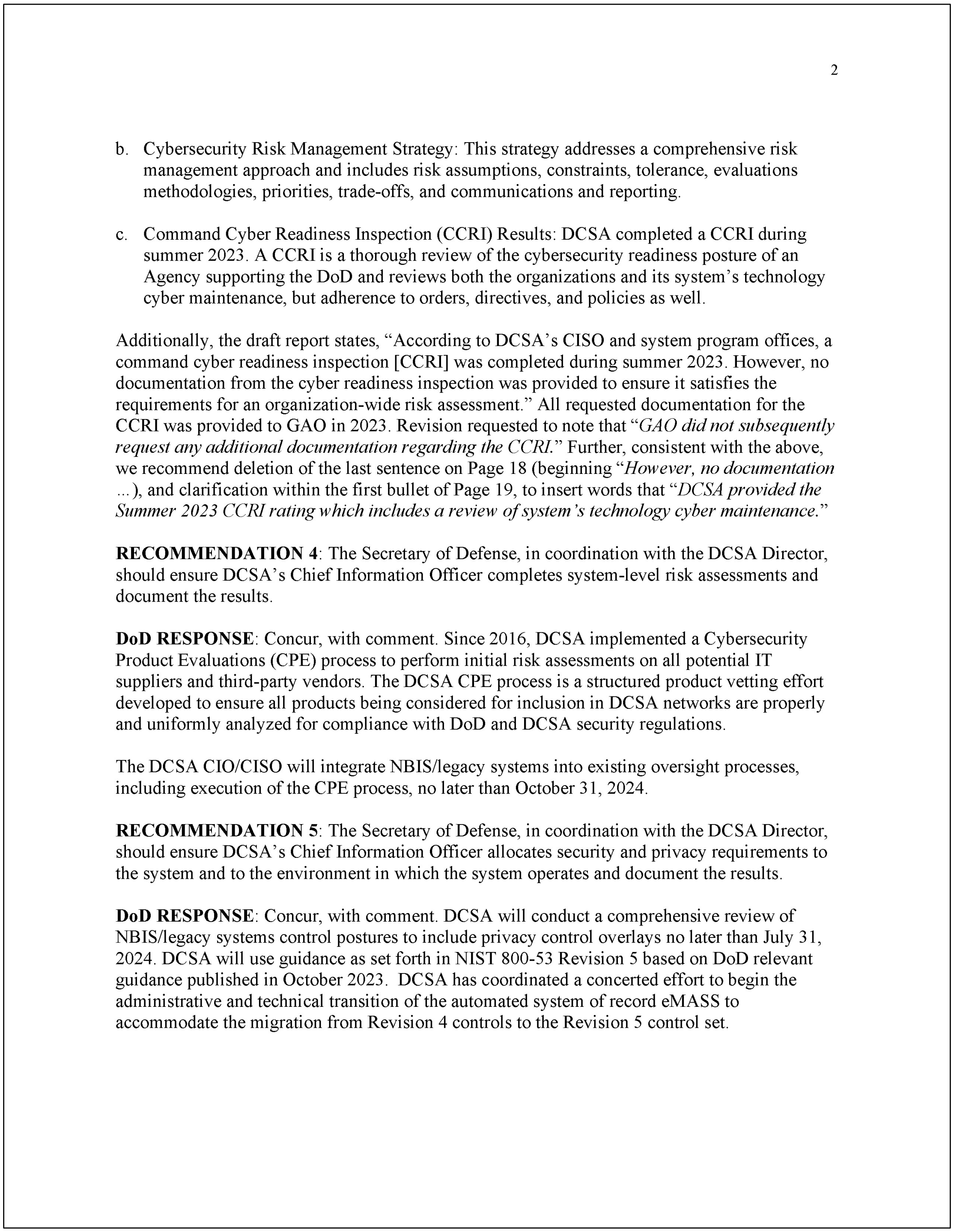
RECOMMENDATION 2: The Secretary of Defense, in coordination with the DCSA Director, should ensure DCSA's Chief Information Officer fully defines, prioritizes, and documents security and privacy requirements.

DoD RESPONSE: Concur, with comment. The DCSA NBIS/legacy system's privacy impact assessments (PIAs) were provided to GAO on December 12, 2023. Five of the six system PIAs were retrieved from eMASS and partially complied with NIST 800-53 Revision 5 requirements. The NBIS Data Management System PIA will be processed and completed by July 31, 2024. DCSA will audit documentation of NBIS/legacy system PIAs by August 30, 2024.

RECOMMENDATION 3: The Secretary of Defense, in coordination with the DCSA Director, should ensure DCSA's Chief Information Officer completes an organization-wide risk assessment and document the results.

DoD RESPONSE: Concur, with comment. DCSA will consolidate documentation supporting the organizational-wide risk assessment task into one product consistent with NIST Cybersecurity Framework (CSF) and DoDI 8510.01 guidance. This updated product will include information obtained from the following documents:

a. AO Risk Assessment Reviews: During an interview with GAO on 3 October 2023, DCSA provided continuing proof of system level updates via monthly reviews with all DCSA System Owners and Program Managers to include NBIS and BIES systems as outlined in section 6 of the Agency Risk Management Strategy.



b. Cybersecurity Risk Management Strategy: This strategy addresses a comprehensive risk management approach and includes risk assumptions, constraints, tolerance, evaluations methodologies, priorities, trade-offs, and communications and reporting.

c. Command Cyber Readiness Inspection (CCRI) Results: DCSA completed a CCRI during summer 2023. A CCRI is a thorough review of the cybersecurity readiness posture of an Agency supporting the DoD and reviews both the organizations and its system's technology cyber maintenance, but adherence to orders, directives, and policies as well.

Additionally, the draft report states, "According to DCSA's CISO and system program offices, a command cyber readiness inspection [CCRI] was completed during summer 2023. However, no documentation from the cyber readiness inspection was provided to ensure it satisfies the requirements for an organization-wide risk assessment." All requested documentation for the CCRI was provided to GAO in 2023. Revision requested to note that "*GAO did not subsequently request any additional documentation regarding the CCRI.*" Further, consistent with the above, we recommend deletion of the last sentence on Page 18 (beginning "*However, no documentation …*), and clarification within the first bullet of Page 19, to insert words that "*DCSA provided the Summer 2023 CCRI rating which includes a review of system's technology cyber maintenance.*"

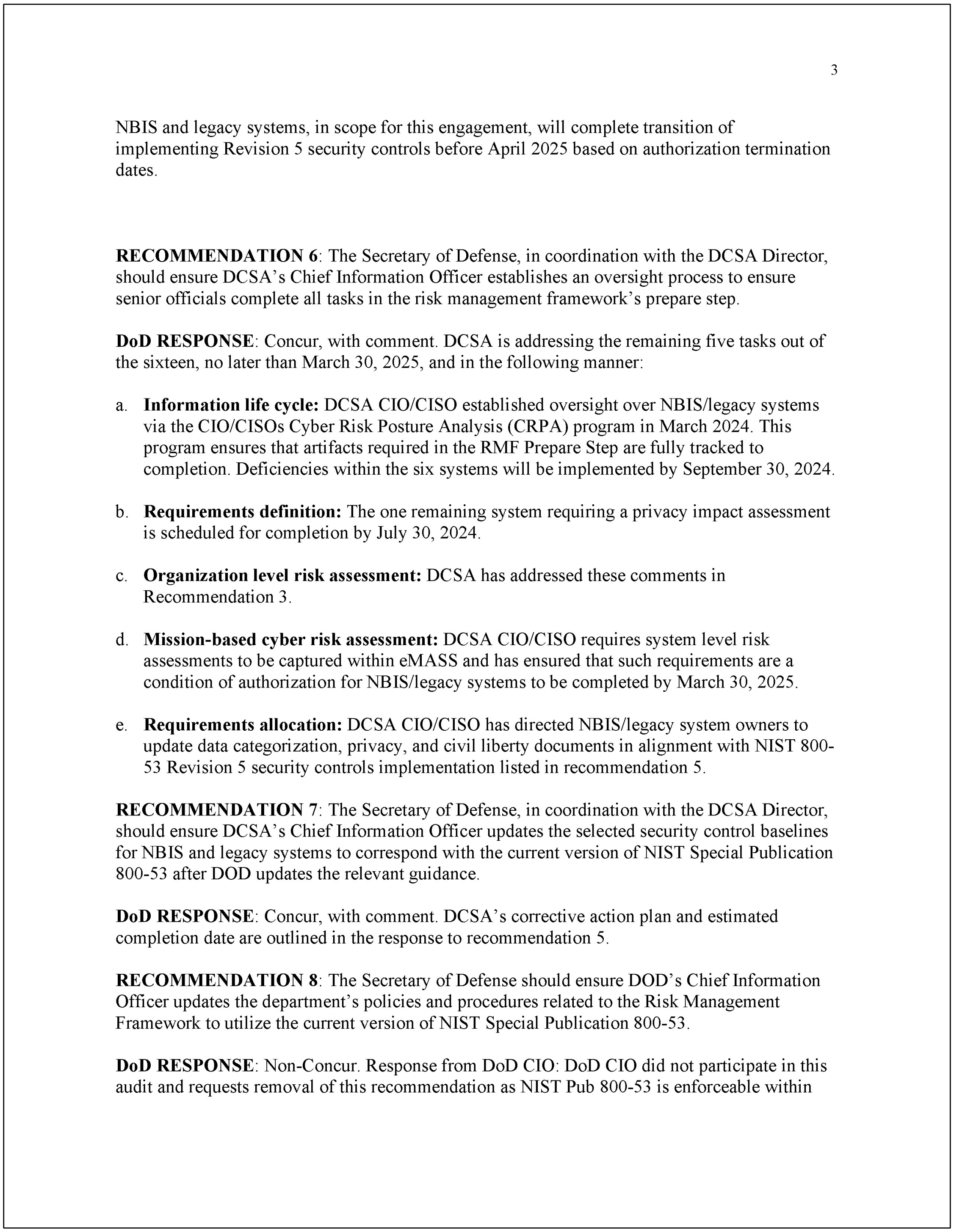
RECOMMENDATION 4: The Secretary of Defense, in coordination with the DCSA Director, should ensure DCSA's Chief Information Officer completes system-level risk assessments and document the results.

DoD RESPONSE: Concur, with comment. Since 2016, DCSA implemented a Cybersecurity Product Evaluations (CPE) process to perform initial risk assessments on all potential IT suppliers and third-party vendors. The DCSA CPE process is a structured product vetting effort developed to ensure all products being considered for inclusion in DCSA networks are properly and uniformly analyzed for compliance with DoD and DCSA security regulations.

The DCSA CIO/CISO will integrate NBIS/legacy systems into existing oversight processes, including execution of the CPE process, no later than October 31, 2024.

RECOMMENDATION 5: The Secretary of Defense, in coordination with the DCSA Director, should ensure DCSA's Chief Information Officer allocates security and privacy requirements to the system and to the environment in which the system operates and document the results.

DoD RESPONSE: Concur, with comment. DCSA will conduct a comprehensive review of NBIS/legacy systems control postures to include privacy control overlays no later than July 31, 2024. DCSA will use guidance as set forth in NIST 800-53 Revision 5 based on DoD relevant guidance published in October 2023. DCSA has coordinated a concerted effort to begin the administrative and technical transition of the automated system of record eMASS to accommodate the migration from Revision 4 controls to the Revision 5 control set.



NBIS and legacy systems, in scope for this engagement, will complete transition of implementing Revision 5 security controls before April 2025 based on authorization termination dates.

RECOMMENDATION 6: The Secretary of Defense, in coordination with the DCSA Director, should ensure DCSA's Chief Information Officer establishes an oversight process to ensure senior officials complete all tasks in the risk management framework's prepare step.

DoD RESPONSE: Concur, with comment. DCSA is addressing the remaining five tasks out of the sixteen, no later than March 30, 2025, and in the following manner:

a. **Information life cycle:** DCSA CIO/CISO established oversight over NBIS/legacy systems via the CIO/CISOs Cyber Risk Posture Analysis (CRPA) program in March 2024. This program ensures that artifacts required in the RMF Prepare Step are fully tracked to completion. Deficiencies within the six systems will be implemented by September 30, 2024.

b. **Requirements definition:** The one remaining system requiring a privacy impact assessment is scheduled for completion by July 30, 2024.

c. **Organization level risk assessment:** DCSA has addressed these comments in Recommendation 3.

d. **Mission-based cyber risk assessment:** DCSA CIO/CISO requires system level risk assessments to be captured within eMASS and has ensured that such requirements are a condition of authorization for NBIS/legacy systems to be completed by March 30, 2025.

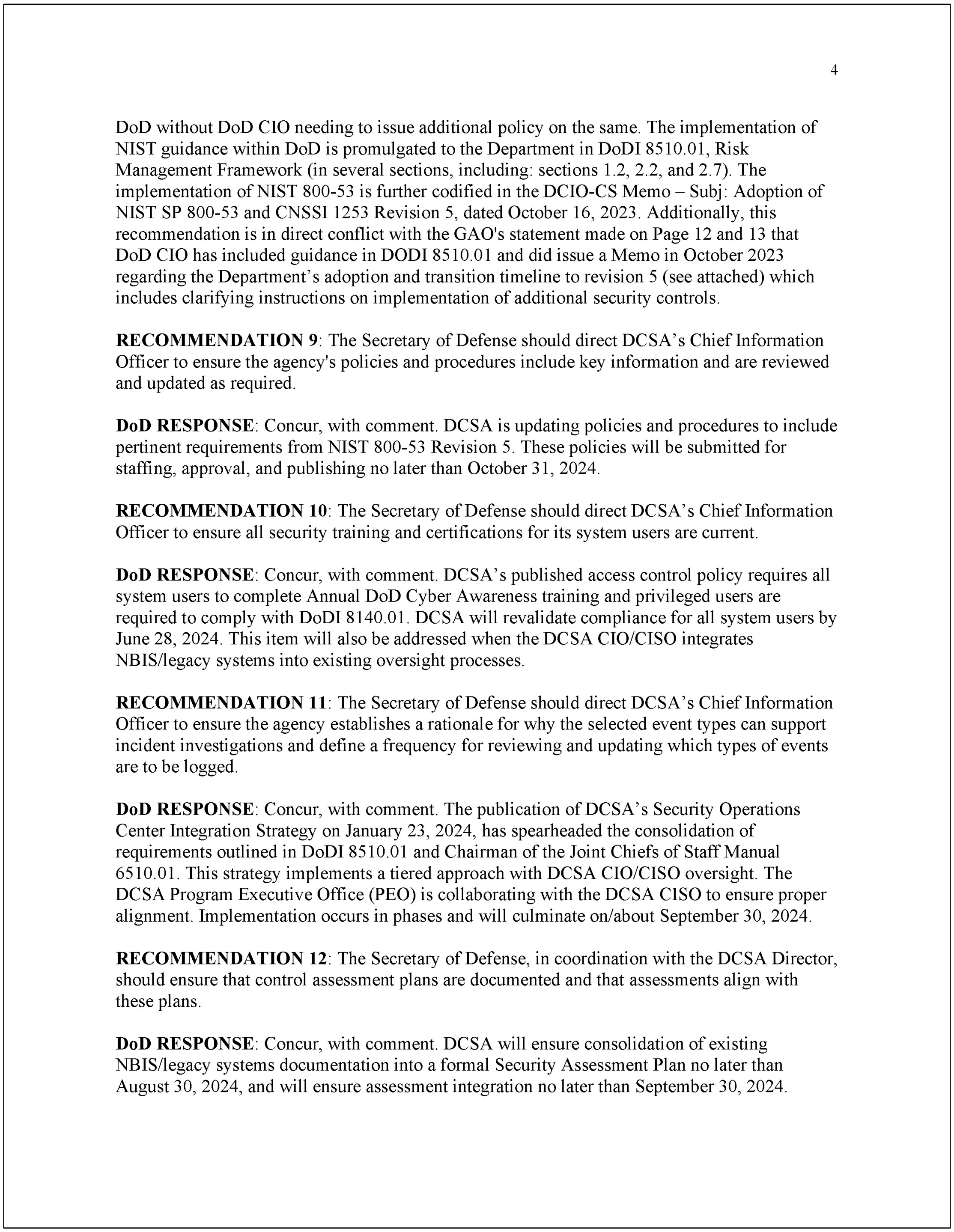
e. **Requirements allocation:** DCSA CIO/CISO has directed NBIS/legacy system owners to update data categorization, privacy, and civil liberty documents in alignment with NIST 800-53 Revision 5 security controls implementation listed in recommendation 5.

RECOMMENDATION 7: The Secretary of Defense, in coordination with the DCSA Director, should ensure DCSA's Chief Information Officer updates the selected security control baselines for NBIS and legacy systems to correspond with the current version of NIST Special Publication 800-53 after DOD updates the relevant guidance.

DoD RESPONSE: Concur, with comment. DCSA's corrective action plan and estimated completion date are outlined in the response to recommendation 5.

RECOMMENDATION 8: The Secretary of Defense should ensure DOD's Chief Information Officer updates the department's policies and procedures related to the Risk Management Framework to utilize the current version of NIST Special Publication 800-53.

DoD RESPONSE: Non-Concur. Response from DoD CIO: DoD CIO did not participate in this audit and requests removal of this recommendation as NIST Pub 800-53 is enforceable within



DoD without DoD CIO needing to issue additional policy on the same. The implementation of NIST guidance within DoD is promulgated to the Department in DoDI 8510.01, Risk Management Framework (in several sections, including: sections 1.2, 2.2, and 2.7). The implementation of NIST 800-53 is further codified in the DCIO-CS Memo – Subj: Adoption of NIST SP 800-53 and CNSSI 1253 Revision 5, dated October 16, 2023. Additionally, this recommendation is in direct conflict with the GAO's statement made on Page 12 and 13 that DoD CIO has included guidance in DODI 8510.01 and did issue a Memo in October 2023 regarding the Department's adoption and transition timeline to revision 5 (see attached) which includes clarifying instructions on implementation of additional security controls.

RECOMMENDATION 9: The Secretary of Defense should direct DCSA's Chief Information Officer to ensure the agency's policies and procedures include key information and are reviewed and updated as required.

DoD RESPONSE: Concur, with comment. DCSA is updating policies and procedures to include pertinent requirements from NIST 800-53 Revision 5. These policies will be submitted for staffing, approval, and publishing no later than October 31, 2024.

RECOMMENDATION 10: The Secretary of Defense should direct DCSA's Chief Information Officer to ensure all security training and certifications for its system users are current.

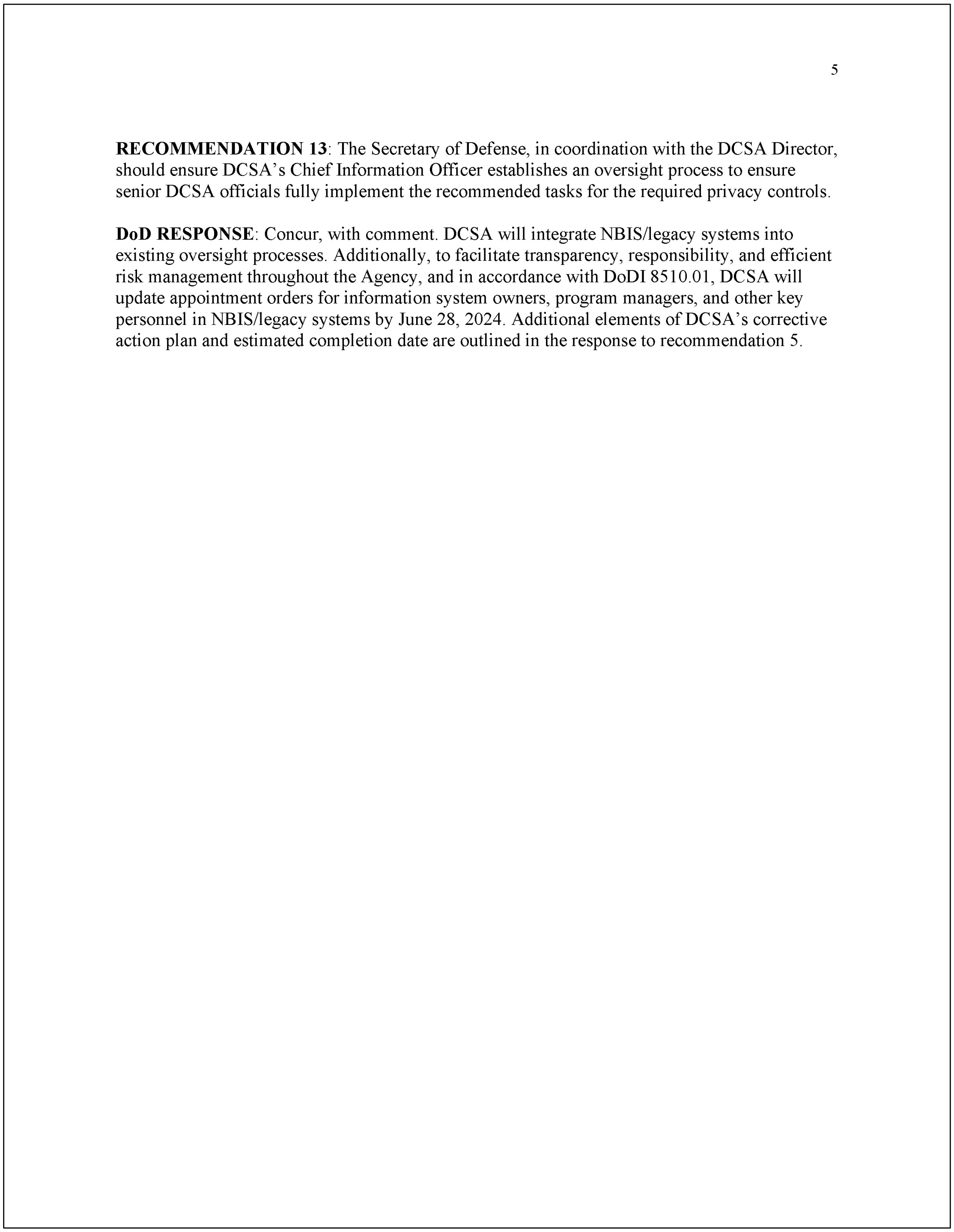
DoD RESPONSE: Concur, with comment. DCSA's published access control policy requires all system users to complete Annual DoD Cyber Awareness training and privileged users are required to comply with DoDI 8140.01. DCSA will revalidate compliance for all system users by June 28, 2024. This item will also be addressed when the DCSA CIO/CISO integrates NBIS/legacy systems into existing oversight processes.

RECOMMENDATION 11: The Secretary of Defense should direct DCSA's Chief Information Officer to ensure the agency establishes a rationale for why the selected event types can support incident investigations and define a frequency for reviewing and updating which types of events are to be logged.

DoD RESPONSE: Concur, with comment. The publication of DCSA's Security Operations Center Integration Strategy on January 23, 2024, has spearheaded the consolidation of requirements outlined in DoDI 8510.01 and Chairman of the Joint Chiefs of Staff Manual 6510.01. This strategy implements a tiered approach with DCSA CIO/CISO oversight. The DCSA Program Executive Office (PEO) is collaborating with the DCSA CISO to ensure proper alignment. Implementation occurs in phases and will culminate on/about September 30, 2024.

RECOMMENDATION 12: The Secretary of Defense, in coordination with the DCSA Director, should ensure that control assessment plans are documented and that assessments align with these plans.

DoD RESPONSE: Concur, with comment. DCSA will ensure consolidation of existing NBIS/legacy systems documentation into a formal Security Assessment Plan no later than August 30, 2024, and will ensure assessment integration no later than September 30, 2024.



RECOMMENDATION 13: The Secretary of Defense, in coordination with the DCSA Director, should ensure DCSA's Chief Information Officer establishes an oversight process to ensure senior DCSA officials fully implement the recommended tasks for the required privacy controls.

DoD RESPONSE: Concur, with comment. DCSA will integrate NBIS/legacy systems into existing oversight processes. Additionally, to facilitate transparency, responsibility, and efficient risk management throughout the Agency, and in accordance with DoDI 8510.01, DCSA will update appointment orders for information system owners, program managers, and other key personnel in NBIS/legacy systems by June 28, 2024. Additional elements of DCSA's corrective action plan and estimated completion date are outlined in the response to recommendation 5.

Appendix III: Contacts and Staff Acknowledgments

GAO Contacts

Jennifer R. Franks, (404) 679-1831 or FranksJ@gao.gov
Alissa H. Czyz, (202) 512-3058 or CzyzA@gao.gov

Staff Acknowledgments

In addition to the individuals named above, the following staff made key contributions to this report: Mark Canter (Assistant Director), Kimberly Seay (Assistant Director), Daniel Swartz (Assistant Director), Ashley Houston (Analyst in Charge), Evelyn Dube, Tarunkant Mithani, Carlo Mozo, Edward Varty, and Andrew Yarbrough. Lauri Barnes, Jonnie Genova, Smith Julmisse, Michael Lebowitz, and Andrew Stavisky also provided support 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

Sarah Kaczmarek, Acting Managing Director, kaczmareks@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