United States Government Accountability Office

Report to the Committee on Armed Services, House of Representatives

June 2021

DEFENSE CYBERSECURITY

Defense Logistics Agency Needs to Address Risk Management Deficiencies in Inventory Systems

Accessible Version

GAO@100
A Century of Non-Partisan Fact-Based Work

GAO-21-278

GAO Highlights

Highlights of GAO-21-278, a report to the Committee on Armed Services, House of Representatives

Why GAO Did This Study

In November 2018 DOD's Survivable Logistics Task Force examined current and emerging threats to DOD logistics, including cybersecurity threats. The task force concluded that DOD's inventory management systems were potentially vulnerable to cyberattacks, and that DOD did not have corrective action plans to mitigate the potential risks posed by associated vulnerabilities.

House Report 116-120, accompanying a bill for the National Defense Authorization Act for Fiscal Year 2020, included a provision for GAO to evaluate DOD's efforts to manage cybersecurity risks to the DOD supply chain. GAO's report determines the extent to which DLA has implemented risk management steps to address cybersecurity risks to its inventory management systems.

GAO selected six systems that DLA officials deemed critical to inventory management operations. GAO reviewed documents, analyzed data, and interviewed officials to determine whether DLA fully addressed, partially addressed, or did not address DOD steps for cybersecurity risk management.

What GAO Recommends

GAO is making five recommendations for DLA to address shortfalls in its critical inventory management systems' adherence to DOD cybersecurity risk management steps. DLA agreed with two and partially agreed with three recommendations. GAO continues to believe all its recommendations are still warranted.

View GAO-21-278 report. For more information, contact Diana Maurer at (202) 512-9627 or MaurerD@gao.gov or Vijay A D'Souza at 202-512-6240 or Dsouzav@gao.gov

June 2021

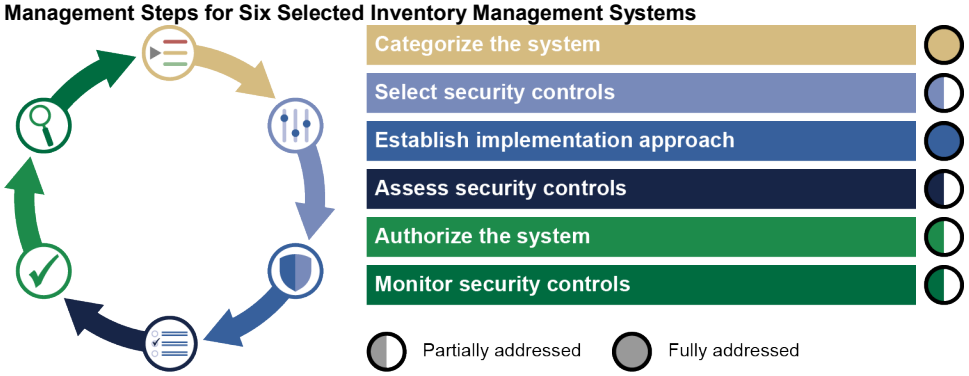
Defense Cybersecurity

Defense Logistics Agency Needs to Address Risk Management Deficiencies in Inventory Systems

What GAO Found

For six selected inventory management systems that support processes for procuring, cataloging, distributing, and disposing of materiel, the Defense Logistics Agency (DLA) fully addressed two of the Department of Defense's (DOD) six cybersecurity risk management steps and partially addressed the other four. Specifically, the agency categorized the systems based on risk and established an implementation approach for security controls. However, it only partially addressed the four risk management steps of selecting, assessing, authorizing, and monitoring security controls (see figure).

Extent to Which the Defense Logistics Agency Addressed the Department of Defense's Risk Management Steps for Six Selected Inventory Management Systems



Source: GAO analysis of Defense Logistics Agency information management inventory systems. | GAO-21-278

- **Select security controls**: DLA selected specific security controls, but it did not develop system-level monitoring strategies to assess the effectiveness of selected security controls for three of the six systems GAO assessed. DOD's risk management framework requires components to develop a system-specific monitoring strategy during the security control selection step.
- **Assess security controls**: DLA assessed the security controls for the six selected inventory management systems, but its assessment procedures lacked approvals, as required. As a result, GAO found that DLA's assessment plans lacked essential details and missed opportunities for risk-based decisions.
- **Authorize the system**: DLA authorized the selected systems, but it did not report complete and consistent security and risk assessment information to support decisions. GAO found that DLA had not established a process for program offices to review authorization documentation prior to submitting packages to the authorizing official.
- **Monitor security controls**: DLA did not consistently monitor the remediation of identified security weaknesses across its six inventory management systems. As a result, GAO found that 1,115 of the 1,627 corrective action plans (69 percent) for the six systems did not complete intended remediation within DLA's required time frame of 365 days or less--they were ongoing for an average of 485 days.

Until DLA addresses the identified deficiencies, the agency's management of cyber risks for critical systems will be impeded and potentially pose risks to other DOD systems that could be accessed if DLA's systems are compromised.

Contents

Figure

Abbreviations

CNSSI	Committee on National Security System Instruction
DLA	Defense Logistics Agency
DOD	Department of Defense
eMASS	Enterprise Mission Assurance Support Service
FISMA	Federal Information Security Modernization Act of 2014
IT	Information Technology
NIST	National Institute of Standards and Technology
RMF	Risk Management Framework

441 G St. N.W.
Washington, DC 20548

June 21, 2021

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

The Department of Defense (DOD) supply chain is a global network that provides materiel, services, and equipment to DOD's joint force. Effective and efficient supply chain management is critical for supporting the readiness and capabilities of the warfighter and the overall success of joint operations. A key aspect of supply chain management is inventory management—the process of determining requirements and procuring, managing, cataloging, distributing, overhauling, and disposing of materiel. The Defense Logistics Agency (DLA), a component of DOD, serves as the nation's combat logistics support agency. DLA and the military services endeavor to provide logistics capabilities to deliver support to the warfighter at the right place, time, and cost. The items that DLA acquires, stores, and distributes to the military services are mostly consumables—that is, items that are normally intended to be used up beyond recovery or repair, such as food, fuel, and spare parts.

To carry out the agency's missions and account for its resources, DLA relies on information systems to access and manage supply chain, inventory, and other logistics data. As such, the security of these systems and data is vital to public confidence and the nation's safety, prosperity, and well-being. However, cyber-based intrusions and attacks on both federal and nonfederal systems have become not only more numerous and diverse, but also more damaging and disruptive. Moreover, the risks to systems supporting the federal government and the nation's critical infrastructure are increasing. Insider threats from witting or unwitting employees, escalating and emerging threats from around the globe, and the emergence of new and more destructive attacks threaten to undermine our utilization of cyber information systems.

In recognition of the growing threat, we designated information security as a government-wide high-risk area in 1997, and it has since remained on our high-risk list. In addition, we recently reported that although the federal government has made some improvements in cybersecurity, it needs to move with a greater sense of urgency to address four major

cybersecurity challenges and 10 associated critical actions commensurate with the rapidly evolving and grave threats to the country.[1]

DOD has also recognized the growing threat to its logistics networks and information systems from adversaries and has established a Task Force to examine current and emerging threats to DOD logistics, including cybersecurity threats.[2] In November 2018 the Task Force concluded that logistics information systems—which include inventory management systems—were potentially vulnerable to cyberattacks, and DOD did not have corrective action plans to mitigate the potential risks posed by associated vulnerabilities.

House Report 116-120, accompanying a bill for the National Defense Authorization Act for Fiscal Year 2020, includes a provision for us to evaluate DOD's efforts to identify, address, and mitigate cybersecurity risks to the DOD supply chain.[3] Our objective was to determine the extent to which DLA has implemented key risk management steps to address cybersecurity risks to its inventory management systems.

To address our objective, we selected six independent inventory management systems, which DLA cybersecurity officials deemed critical to their inventory management operations, to examine. We reviewed DOD's instruction on cybersecurity risk management (also referred to as the DOD risk management framework)[4] to identify six risk management steps. Next, we reviewed DLA's cybersecurity policies and guidance, as well as documentation on DLA's authorization to operate these six

[1]GAO, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, GAO-21-288 (Washington, D.C.: Mar. 24, 2021).

[2]Department of Defense (DOD), *Final Report of the Defense Science Board (DSB) Task Force on Survivable Logistics*, (November 2018).

[3]H.R. Rep. No. 116-120, at 309-10 (2019).

[4]DOD Instruction 8510.01, *Risk Management Framework (RMF) for DOD Information Technology (IT)*, (March 12, 2014) (incorporating Change 2, July 28, 2017). DOD revised this instruction in December 2020 but did not include any substantive changes to the steps that we evaluated at the system level. We did not use the updated version of this guidance in our review, because we focused on the agency's risk management framework actions from 2018 to 2019 system authorizations.

selected inventory management systems.[5] The six select systems were authorized between May 2018 and November 2019 and were the most recent authorizations to operate during our review, which began in September 2019. [6]

In addition, we obtained and analyzed documents used by DLA cybersecurity officials to implement, oversee, and demonstrate compliance with risk management steps.[7] We also reviewed timeliness and risk data from DOD's information technology (IT) tool for managing the risk management framework—the Enterprise Mission Assurance Support Service, hereinafter referred to as eMASS—to assess the six DLA program offices' efforts to implement these risk management steps.[8]

To assess the reliability of data obtained from eMASS, we interviewed knowledgeable officials in the agency's Cybersecurity Office and the six system program offices about the quality control procedures used to ensure the accuracy and completeness of the data. We also compared the data with other relevant documentation on each system's security controls. We found that most of the security control data we examined were sufficiently reliable for evaluating DLA's risk management steps for the selected inventory management systems. We note below where discrepancies in the data impacted the system program offices' ability to address DOD's risk management steps.

We evaluated DLA's documents and the eMASS data against requirements from the six risk management steps identified in (1) DOD's risk management framework and supplemental risk guidance and (2)

[5]Prior to an information system's being allowed to operate on DOD's information network, a senior organizational official must authorize operation of the system and explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation, based on the implementation of an agreed-upon set of security controls. According to DOD guidance, every 3 years a senior organizational official must determine whether to re-authorize the system to remain operational on the network.

[6]We do not name the six systems in relation to any assessment results. This information is considered controlled unclassified information and cannot be publicly released.

[7]Where available, DLA 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.

[8]DLA uses the Enterprise Mission Assurance Support Service (eMASS), which is managed by the Defense Information Systems Agency, as its tool for supporting the implementation of risk management framework steps.

DLA's related standard operating procedures.[9] In addition, we evaluated DLA's efforts against certain guidance identified in the National Institute of Standards and Technology's (NIST)[10] and from the Committee on National Security System Instruction (CNSSI) No. 1253,[11] because DOD's instruction directs DLA to also comply with these documents. We supplemented our analysis of documents and observations by interviewing officials in DLA's Cybersecurity Office and the six system program offices about their efforts to assess, document, and review security controls for their respective systems. We then made determinations about the extent to which each system's program office had fully addressed, partially addressed, or did not address all aspects of the required tasks for the risk management step, based on the documentation and data provided.

This report does not address the extent to which DLA and the selected systems' countermeasures are able to successfully prevent certain cyberattacks. Rather, it focuses on DLA's efforts to manage the cybersecurity of these six systems through a risk management framework that is intended to help managers make informed decisions about cyber threats, and to prioritize mitigations and responses to threats in the most cost-effective manner.

We have included key concept boxes throughout the report to assist the reader's understanding of cybersecurity terminology. These concepts are not formal definitions of these terms but are based on our analysis of

[9]DOD Instruction 8510.01; DOD, *Program Managers Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle*, (September 2015 Version 1); Defense Logistics Agency, Standard Operating Procedure, 8510.01-01, *DLA Risk Management Framework (RMF)* (Sept. 25, 2018).

[10]National Institute of Standards and Technology (NIST) Special Publication 800-53A, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*, Revision 4 (December 2014).

[11]Committee on National Security Systems Instruction (CNSSI) No. 1253, *Security Categorization and Control Selection for National Security Systems* (Mar. 27, 2014). Although the six systems in this report are critical to DLA operations, these systems are not national security systems. 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 (CNSSI) No. 1253. This guidance builds on and is a companion document to NIST guidance relevant to categorization and selection.

various publications from CNSS, DOD, and DLA, and NIST publications.[12] DOD uses various sources to define its cybersecurity terms, including CNSS and NIST publications.[13]

We conducted this performance audit from September 2019 to June 2021 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. We discuss our scope and methodology in more detail in appendix I.

Background

DOD's supply chain is a global network that provides materiel, services, and equipment to U.S. military forces. Inventory management is the process of determining requirements and acquiring, managing, cataloging, distributing, overhauling, and disposing of materiel. Management and oversight of DOD's inventory are a responsibility shared among the Under Secretary of Defense for Acquisition and Sustainment, DLA, and the military services. Specifically, DLA acquires, stores, and distributes mostly consumable items—those that are normally expended or intended to be used up beyond recovery or repair—and

[12]For example, National Institute of Standards and Technology (NIST), *Risk Management Framework for Information Systems and Organizations,* Special Publication 800-37, Revision 2 (Gaithersburg, Md.: December 2018); Committee on National Security Systems Instruction (CNSSI) No. 1253, *Security Categorization and Control Selection for National Security Systems* (Mar. 27, 2014); DOD Instruction 8510.01; DOD, *Program Managers Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle*, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (September 2015 Version 1); and Defense Logistics Agency, Standard Operating Procedure, 8510.01-01, *DLA Risk Management Framework (RMF)* (Sept. 25, 2018).

[13]For example. National Institute of Standards and Technology (NIST), Glossary, May 2021, https://csrc.nist.gov/glossary; and Committee on National Security Systems Instruction (CNSSI) No. 4009, *Committee on National Security Systems (CNSS) Glossary* (April 6, 2015). For a more complete list of cybersecurity terms, see DOD 8510.01.

provides these items to the military services when requisitioned in support of approximately 2,400 weapon systems.[14]

Overview of DLA Inventory Management Systems

The six DLA information systems we assessed are critical to the agency's inventory management operations. These systems support the management of supply, transportation, and fuel data. Table 1 describes the six selected systems and shows the date of authorization for which each received approval or authorization to operate on the DOD network.

Table 1: Defense Logistics Agency (DLA) Systems Assessed by GAO as Critical to Inventory Management Operations

System	Description	Date of Authorization
Base Level Support Application/Fuels Manager Defense	Provides information on fuel consumption at forward-deployed locations and can assist a base commander in making decisions regarding energy use on the base.	September 2019
Defense Automatic Addressing System	Maintains, for military activities, federal agencies, and contractors, the "activity address codes"—that is, the codes used to provide a uniform method for controlling government assets and recording the receipt and disposition of property.	February 2019
Distribution Standard System	Manages functional business processes of DLA's warehouse operations, to include receiving, storage, packing, shipping, inventory inspection, and workload management.	October 2018
Federal Logistics Information System	Catalogs the national stock numbers assigned to items that are repeatedly acquired, purchased, stocked, stored, issued, and used throughout the federal supply system.	June 2018
Hazardous Material Management System	Provides information about who received hazardous materials; which and how much they received; and when, where, and how the materials were used.	November 2019
Wide Area Workflow E-Business Suite	Provides means for electronic submission, acceptance, and processing of invoices and receiving reports, and for matching them with contracts to authorize payment.	May 2018

Source: GAO analysis of DLA information. | GAO-21-278

[14]For additional information on DLA's inventory management steps see GAO, *Defense Inventory: Actions Needed to Improve the Defense Logistics Agency's Inventory Management,* GAO-14-495 (Washington, D.C.: June 19, 2014)

Cybersecurity Risk Management

For DLA, as for all government organizations, cybersecurity is a key element in maintaining public trust. Inadequately protected systems pose risks to the protection of information, privacy, and military operations. As we have previously reported, unintentional, or non-adversarial, threat sources include equipment failures, software coding errors, or the accidental actions of employees (human errors). Systems are also vulnerable to individuals or groups with malicious intent who could unlawfully access the systems to obtain sensitive information, disrupt operations, or launch attacks against other computer systems and networks.

Key Concept

Common terminology for cybersecurity risk management can include:

- A cyber vulnerability is a weakness in an information system that could be exploited or otherwise affected by a threat.
- A cybersecurity threat is anything that can potentially harm a system, either intentionally or unintentionally.

A cybersecurity risk assessment is a measurement of the potential effect posed by a threat (intent and capabilities), a vulnerability (inherent or introduced) to a threat, and potential consequences (fixable or fatal).

Source: GAO analysis of NIST information. | GAO-21-278

Cybersecurity risk management comprises a full range of activities undertaken to protect IT and data from unauthorized access and other cyber threats; maintain awareness of cyber threats; detect anomalies and incidents adversely affecting IT and data; and mitigate the impact of, respond to, and recover from incidents.

Federal law and guidance specify requirements for protecting federal information and information systems. The Federal Information Security Modernization Act of 2014 (FISMA) requires executive branch agencies to develop, document, and implement agency-wide programs to provide security for the information and information systems that support their operations and assets.[15] NIST is tasked with the mission of developing, for systems other than those for national security, standards and guidelines to be used by all agencies to establish minimum cybersecurity requirements for information and information systems based on their respective levels of cybersecurity risk.[16] Accordingly, NIST developed a risk management framework of standards and guidelines for agencies to follow when developing information security programs.

[15]The Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 2014), updated and largely superseded the Federal Information Security Management Act of 2002, Pub. L. No. 107-347(2002). As used in this report, FISMA refers to the requirements in the 2014 law.

[16]15 U.S.C. § 278g-3(a) and (b).

Key Concept

Security controls are safeguards or countermeasures to protect the confidentiality, integrity, and availability of a system and its information. For example, the system owner may add encryption as a safeguard to protect confidentiality by transforming information so that only authorized users are able to read it, and may protect integrity by providing the safeguard of an electronic signature that can be used to check for unauthorized changes to the file. System owners can also back up data routinely as a countermeasure to help ensure availability in the event of a disruption or failure.

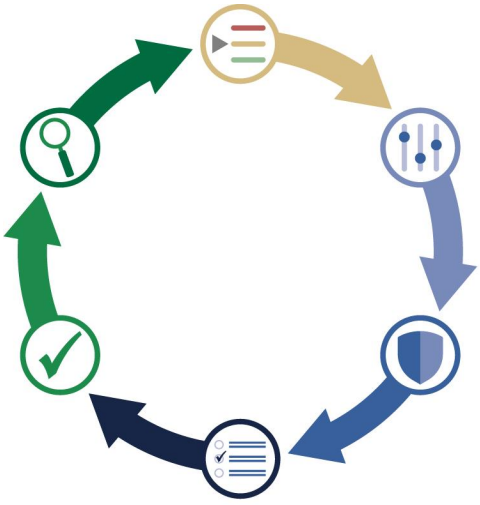
Source: GAO analysis of NIST information. | GAO-21-278

DOD's Office of the Chief Information Officer has also established a series of policies, procedures, and guidance to defend its information systems and computer networks from unauthorized or malicious activity and ensure their security. For example, DOD Instruction 8510.01, *Risk Management Framework (RMF) for DOD Information Technology (IT)*, describes the department's requirements for executing and maintaining the risk management framework for its IT systems.[17] The cybersecurity requirements outlined in DOD's framework are intended to be consistent with NIST standards and guidelines and consist of six steps: (1) categorizing the system's impact level; (2) selecting security controls; (3) implementing security controls; (4) assessing security controls; (5) authorizing the system to operate; and (6) monitoring the efficacy of controls on an ongoing basis.[18] Figure 1 shows an overview of this framework and describes its six steps. These steps are to be typically implemented in a cyclical approach when seeking authorization for a new or unauthorized system. Once authorized to operate, a system must be reassessed and reauthorized every 3 years.

[17]DOD Instruction 8510.01.

[18]NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations,* Revision 2 (December 2018) adds an additional "Prepare" step in order to establish the context and priorities for managing security and privacy risk at both the organizational level and the system level. The current DOD Risk Management Framework does not include this step, although DOD officials told us that they are updating DOD Instruction 8510.01 in order to do so. As such, we did not include this step in our review.

Figure 1: Overview of the Department of Defense's (DOD) Cybersecurity Risk Management Framework for Information Technology (IT) Systems



Categorize the system

Categorize the information system in accordance with national security guidance[a] and document the results in the security plan. The categorization process identifies the system 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 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 system

Provide, through a designated official, the Authorization to Operate, which certifies the system 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 system on an ongoing basis, including assessing control effectiveness, conducting planned remediation activities, and reporting the security state of the system to designated officials.

Source: GAO analysis of Department of Defense (DOD) guidance. | GAO-21-278

Text of Figure 1: Overview of the Department of Defense's (DOD) Cybersecurity Risk Management Framework for Information Technology (IT) Systems

- **Categorize the system:** Categorize the information system in accordance with national security guidance/a/ and document the results in the security plan. The categorization process identifies the system 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 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 system:** Provide, through a designated official, the Authorization to Operate, which certifies the system for operation based on complete assessment of security controls, remedial actions and acceptance of residual risks to organizational operations.
- **Monitor security controls:** nitor the security controls in the information system on an ongoing basis, including assessing control effectiveness, conducting planned remediation activities, and reporting the security state of the system to designated officials.

Source: GAO analysis of Department of Defense (DOD) guidance. | GAO-21-278

Note: While the risk management framework steps are listed in sequential order in the figure, the steps can be carried out in a nonsequential order. 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. However, there could be many points in the risk management process where there is a need to diverge from the sequential order due to the type of system, risk decisions made by senior leadership, or changes in risk or in system functionality, or to allow for iterative cycles between tasks or revisiting of tasks (e.g., during agile development).

[a]Committee on National Security Systems Instruction (CNSSI) No. 1253, Security Categorization and Control Selection for National Security Systems (March 27, 2014).

The DOD framework—issued in March 2014—replaced the DOD Information Assurance Certification and Accreditation Process and manages the life-cycle cybersecurity risk to DOD IT. In 2017, DLA issued guidance to the new risk management framework. Management and oversight of the DLA cybersecurity risk management framework program are a responsibility of DLA's Cybersecurity Office. Specifically, the DLA Cybersecurity Office establishes the policy for DLA cybersecurity management and manages the risk management framework process, among other things. In September 2018, the DLA Cybersecurity Office established a standard operating procedure to govern its programs in conducting, implementing, and maintaining the DOD risk management framework.[19]

[19]DLA Standard Operating Procedure 8510.01-01.

DLA Fully Addressed Two of Six Key Risk Management Steps to Address Cybersecurity Risks and Partially Addressed Four Others

DLA fully addressed two of the six key risk management steps by categorizing the systems based on risk and implementing security controls for each of the six selected systems. However, the agency only partially addressed the other four risk management steps of selecting security controls, assessing, authorizing, and monitoring for each of the six selected systems. Table 2 summarizes our assessment of the extent to which DLA addressed each step based on documents and data supporting the authorization of the six selected systems.

Table 2: Extent to Which the Defense Logistics Agency Addressed the Department of Defense's Key Risk Management Steps for Six Selected Inventory Management Systems

Key risk management steps		GAO assessment
1.	Categorize system	Fully addressed
2.	Select security controls	Partially addressed
3.	Establish implementation approach	Fully addressed
4.	Assess security controls	Partially addressed
5.	Authorize system	Partially addressed
6.	Monitor security controls	Partially addressed

Source: GAO analysis of Defense Logistics Agency data and Department of Defense's risk management framework. | GAO-21-278

DLA Categorized the Six Selected Systems and Established an Approach to Implement Security Controls

DLA Categorized the Systems

For the six selected inventory management systems, DLA program offices fully addressed the key risk management step of system categorization. DLA programs are required to categorize their information systems in accordance with CNSSI No. 1253.[20] Furthermore, DLA programs are to select protective measures, or security controls, based on the system categorization results, and to plan for the implementation of these security controls in the system security plan. Each program office documented in its system security plan the various types of data and information the system would process, store, transmit, or protect.

Based on the information types, the DLA program offices assigned a low-, moderate-, or high-security impact level in the areas of the confidentiality, availability, and integrity of each system using the recommended levels identified by NIST and other risk factors, as required by CNSSI guidance.[21] This allowed DLA's programs to determine the extent to which threats could adversely impact the organization and the extent to

[20]As previously mentioned, 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 CNSSI No. 1253.

[21]Committee on National Security Systems Instruction (CNSSI) No. 1253, Security Categorization and Control Selection for National Security Systems (Mar. 27, 2014).

which agency systems are vulnerable to these circumstances or events. Categorizing the system directly impacts the other steps in the framework, from selecting security controls to defining the level of effort in assessing security control effectiveness. An incorrect impact analysis on the risks to confidentiality, integrity, and availability could result in the agency's either over-protecting the system and wasting valuable security resources, or under-protecting the information system and placing important inventory management operations and assets at risk of compromise. Table 3 shows the assigned impact levels for the six selected inventory management systems.

Table 3: Assigned Impact Levels for the Six Selected Defense Logistics Agency (DLA) Inventory Management Systems

System	Confidentiality	Integrity	Availability
System A	Low	Moderate	Low
System B	Low	Moderate	Low
System C	Low	Moderate	Moderate
System D	Moderate	Moderate	Low
System E	Moderate	Moderate	Low
System F	Moderate	Moderate	Moderate

Source: GAO analysis of DLA data.| GAO-21-278

Note: We do not name the six systems in relation to the risk management steps. This information is considered controlled unclassified information and cannot be publicly released.

DLA Established Its Approach to Implement Security Controls

Following the security categorization process, DLA selected security controls for the six inventory management systems (as further discussed later in this report) and established its approach to implement selected controls in each system's security plan.[22] The plans to implement those controls were based on guidance from DOD's online risk management portal, known as the DOD Knowledge Service.[23] Consistent with DOD guidance, these plans describe actions DOD should take for each

[22]DLA inventory management systems meet some security control requirements through inherited controls. DLA identified the inherited security controls in its system security plans and documented the associated inherited compliance status in the security assessment reports for each of the six selected inventory management systems.

[23]DOD's Knowledge Service is an online knowledge base that supports the risk management framework implementation, planning, and execution by functioning as the authoritative source for the risk management framework procedures and guidance. It also provides access to DOD security control baselines, security control descriptions, security control overlays, implementation guidance, and assessment procedures.

security control that will be applied to an IT system. For example, the guidance instructed programs on how to implement a control to prevent unsuccessful log-in attempts. As part of this control, programs were to define the circumstances—such as number of unsuccessful attempts, time period between attempts, or lock-out time period—under which the information system is to delay additional log-in attempts or automatically lock the user account after failed attempts to enter a password.

By categorizing its system and establishing an approach to implement selected security controls, DLA took initial steps to protect the six selected systems and other DOD systems that could be accessed if a malicious cyber actor compromised DLA's systems.

DLA Partially Addressed Selecting Security Controls, Assessing Security, Authorizing Systems, and Monitoring Ongoing Risk

DLA partially addressed the other four risk management steps—selecting security controls, assessing security controls, authorizing systems, and monitoring controls for ongoing risks—for the six selected inventory management systems, as detailed below:

- DLA selected specific security controls, but the agency did not develop monitoring strategies to assess the effectiveness of these controls—as called for during this stage of DOD's risk management framework—for three of the six systems, and only partially developed a monitoring strategy for two of the six systems we assessed.[24]
- DLA assessed the security controls for the six selected inventory management systems, but the assessment procedures lacked approvals from the designated authorizing officials, as required.
- DLA authorized the selected systems, but the agency did not consistently document complete and reliable security and risk assessment information to support its authorization decisions.
- DLA did not consistently monitor the remediation of identified security weaknesses across its six inventory management systems.

[24]In DOD's risk management framework, components are supposed to develop a system-specific strategy for monitoring control effectiveness during the security control selection step.

DLA Selected Security Controls for Each System but Did Not Develop Strategies to Monitor Control Effectiveness

DLA selected specific security controls, but the agency did not develop monitoring strategies to assess effectiveness of these controls for three of the six systems and only partially developed a monitoring strategy for one of the six systems we assessed.

DOD's risk management framework states that during the select security controls step, programs are to select controls for an IT system that are based on its security categorization. In addition, DOD's guidance states that during this step programs are to develop a system-level strategy for the continuous monitoring of the effectiveness of security controls employed within or inherited by the system, and for the monitoring of any proposed or actual changes to the system and its environment of operation.[25]

In addition, DOD's risk management framework states that the cybersecurity requirements for DOD information technologies are to be managed consistent with the principles established in NIST Special Publication 800-37, which provides additional standards and guidelines to federal agencies for cybersecurity risk management. Those principles include ensuring that the system-specific monitoring strategy identifies the system's monitoring frequency, defines the ongoing control assessment approach, describes how ongoing assessments are to be conducted, and defines the reporting requirements.[26]

Each of the DLA program offices selected specific security controls for their respective IT systems based on the impact levels assigned to them in the system categorization step. For example, for two of the six systems—categorized as low-impact for confidentiality and availability and as moderate-impact for integrity—DLA officials selected a baseline of about 375 controls. For one of the six systems—categorized as moderate-impact for confidentiality, integrity, and availability—DLA officials selected a baseline of 403 controls.

[25]DODI 8510.01.

[26]NIST SP 800-37, Revision 2.

Key Concept

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.

Overlays are specific security controls, enhancements, or supplemental guidance intended to complement and refine a system's baseline security controls.

Source: GAO analysis of CNSSI information. | GAO-21-278

As part of their control selection process, each of the DLA program offices determined whether they needed to further customize the baseline security controls by applying overlays or additional controls to enhance the security of their systems. The total number of controls selected for each system varies based on the baseline controls and overlays applied—ranging from about 380 to 450 controls. For example, two of the six systems selected one or more controls that were not required, in an effort to enhance security. Three other systems selected a privacy control overlay to help safeguard personally identifiable information stored or processed by the system.[27]

However, DLA did not develop monitoring strategies, as called for by DOD requirements and related NIST guidance, during this step of the risk management framework. One of the six program offices developed a separate continuous monitoring strategy for its system. Two of the six program offices partially developed system-level monitoring strategies by providing information on the frequency with which systems are monitored, whether the monitoring is manual or automated, and how monitoring results are reported in the eMASS system. While the programs provided useful information regarding their risk monitoring efforts, however, DLA's monitoring strategies did not fully meet DOD requirements and related NIST guidance because they did not sufficiently describe how the effectiveness of security controls would be monitored on a continual basis. Specifically, the strategies did not define the ongoing control assessment approach and did not describe how ongoing assessments are to be conducted.[28] In addition, the other three program offices did not develop any system-level strategy—either in eMASS or as a separate plan.

According to DLA cybersecurity officials, DLA did not require program offices for the six systems we reviewed to have system-level strategies because the enterprise-wide DLA standard operating procedures serve as the system-level monitoring strategy. However, the DOD risk

[27]Personally identifiable information is any information that can be used to distinguish or trace an individual's identity. For example, it can include a name, date and place of birth, Social Security number, or other types of personal information that can be linked to an individual, such as medical, educational, financial, and employment information.

[28]According to NIST, defining the ongoing assessment approach includes activities such as the reuse of assessment procedures and results that supported the initial authorization decision or the analysis of historical and operational data. Additionally, describing how ongoing assessments are to be conducted includes activities such as the use and management of automated tools or instructions for manual monitoring efforts.

management framework and the DLA standard operating procedures in effect when these six systems went through authorization did require a separate continuous monitoring strategy for each system. When DLA subsequently updated its standard operating procedures in April 2020, the agency revised this requirement and stated that the enterprise-wide procedures would also serve as the system-level monitoring strategies for DLA.

DLA's current standard operating procedures for cybersecurity, which emphasize an enterprise-wide monitoring strategy in the absence of system-level monitoring strategies, conflict with the requirements and intent of DOD's risk management framework. An official from DOD's Risk Management Framework Task Advisory Group stated that although an organization can monitor security at the enterprise level, some aspects of security have to be monitored and managed at the system level. According to the official, the policies and procedures that guide a user's behavior on a system generally have to be managed and monitored at the system level, and would not be effective at the enterprise level.

DLA's standard operating procedures are also inconsistent with NIST recommendations for developing system-specific monitoring strategies. In particular, DLA's standard operating procedures do not address the elements that call for defining the ongoing control assessment approach and describing how ongoing assessments are to be conducted for individual systems. Such details are important for ensuring that the effectiveness of a system's controls are monitored through appropriate methods and with a level of rigor commensurate with the risk of harm from the loss of confidentiality, integrity, or availability of information controlled by a system.

Until DLA revises its standard operating procedures to be consistent with the DOD risk management framework and NIST guidance for establishing monitoring strategies during the control selection step, DLA management may be unable to fully understand the security posture of its systems and the effectiveness of controls implemented. Additionally, DLA may be at greater risk of unnecessarily exposing its inventory management programs to increased exploitation.

DLA Assessed Security Controls, but Assessment Plans Lacked Approvals

DLA's security assessment team assessed the implementation of the selected security controls to determine whether they were compliant (i.e.,

implemented in accordance with defined requirements) or non-compliant (i.e., not implemented in accordance with defined requirements). Table 4 identifies the number of compliant and non-compliant controls for each inventory management system according to the system security assessment reports.

Table 4: Number of Compliant and Non-compliant Controls, as Identified by the Defense Logistics Agency's Controls Assessment, for Each of the Inventory Management Systems

System	Number of compliant controls	Number of non-compliant controls
System A	312	109
System B	282	68
System C	374	11
System D	389	39
System E	304	66
System F	324	17
TOTAL	**1,985**	**310**

Source: GAO analysis of Defense Logistics Agency data. | GAO-21-278

However, the designated authorizing officials for the six inventory management systems did not review and approve assessment plans before the assessments were conducted. According to DLA officials, the designated authorizing officials reviewed and approved the assessment plans and results as part of the authorization package. However, the authorization package was reviewed and approved after the assessments were completed.

As a result, DLA's assessment plans lacked essential details and missed opportunities for risk-based decisions. For example, DLA did not document the purpose of its assessment efforts, identify what was being assessed, or describe how the assessment team would conduct the assessment, consistent with DOD's definition of a security assessment

plan.[29] Additionally, DLA did not tailor its assessment procedures to address the specific inventory management systems.[30]

Key Concept

An **authorizing official** is a senior federal official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk. The official determines whether the risks to organizational operations, organizational assets, individuals, and other organizations are acceptable.

Source: GAO analysis of NIST information. | GAO-21-278

DOD's risk management framework requires authorizing officials to review and approve assessment plans prior to conducting the assessment. DOD's supplementing risk management guidance on DOD's online risk management portal states that the assessment plans are intended to help the authorizing official establish the appropriate expectations for the control assessment, determine the level of effort needed, and help ensure that an appropriate level of resources are applied to determine security control effectiveness.

DLA cybersecurity officials acknowledged that the designated authorizing officials for the six selected systems did not review and approve assessment plans before the assessments were conducted. Specifically, they told us that the security assessment plan approval process was completed during the system authorization prior to DLA's transition to the DOD risk management framework. According to these officials, DLA plans to revise the DLA standard operating procedures to require the assessment plan approval through the eMASS system. They said that they believe this policy update—expected to be implemented in December 2021—will allow program offices to obtain assessment plan approval from the designated authorizing official prior to assessing the security controls.

However, until DLA revises and implements its system assessment plan approval process to require review and approval before assessments are conducted, the authorizing official may not have adequate and timely visibility to ensure that DLA's planning efforts were sufficient and that its inventory management systems were appropriately assessed. These planning efforts impact the outcome of the control assessment and

[29]DOD's supplementing risk management guidance states that an assessment plan provides the objectives for the security control assessment and a detailed roadmap of how to conduct the assessment.

[30]According to NIST, tailoring provides organizations with the flexibility needed to meet specific organizational requirements and avoid overly constrained assessment approaches. Such tailoring includes modifying or selecting assessment procedures—including making adjustments to baseline procedures where needed—with the appropriate methods and rigor specific to the system. When implemented effectively, tailoring can provide increased confidence that the control was implemented correctly, operating as intended, and able to support continuous improvement to the control's effectiveness.

support the authorizing official's decision to accept system risk and connect the system to DOD's network.

DLA Authorized Its Systems to Operate, but Security Authorization Documents Were Inconsistent and Incomplete

DLA developed security authorization packages for each of the six selected inventory management systems. Consistent with DOD risk management framework guidance, each package consisted of a security assessment report, risk assessment report, and set of corrective action plans (described in table 5).[31] In addition, the eMASS system showed that the respective authorizing officials for all six inventory management systems reviewed and approved these documents in support of all six authorization decisions.

Table 5: Selected Required Documents for a Security Authorization Package for Defense Logistics Agency (DLA) Systems

Document	Description
Security assessment report	Documents the individual control weaknesses, associated risks, and recommendations from the security control assessment. This report should include key information such as issue, issue severity, recommendations, and residual risk for all non-compliant controls.
Risk assessment report	Documents the residual risk of all security controls that were not implemented as required. This report should include key information such as threat, likelihood, potential impact, and mitigations.
Corrective action plan	Describes actions and timelines for addressing security weaknesses outlined in the security assessment report.

Source: GAO analysis of DLA standard operating procedure for implementing the DOD risk management framework. Defense Logistics Agency, Standard Operating Procedure 8510.01-01, DLA Risk Management Framework (RMF), (Sept. 25, 2018). | GAO-21-278

However, these authorization packages did not always include consistent and complete information to support this decision, as required. For example,

- DLA inconsistently reported the security control assessment results (i.e., compliant or non-compliant) in the security assessment reports for four of the six selected inventory management systems. For example, a security assessment report denoted a security control that could mitigate an insider threat as "compliant"; however, during our review of the report, we observed that it noted that the control did not meet all of the criteria identified in the assessment. According to DLA

[31]For the purpose of this report, corrective action plans refer to the plans of actions and milestones that result from the assessment and continuous monitoring of security controls.

officials, all criteria must be met for a security control to be deemed compliant.

Key Concept

Risk assessments rely upon well-defined risk attributes:

- **Likelihood,** which reflects the probability that a specific vulnerability is susceptible to attack.
- **Impact,** a description of the magnitude of effect to the system and organization if a threat were to occur.
- **Mitigations**, which are actions taken to reduce risk.
- **Residual risk** is the combination of likelihood and impact and describes potential risk after all IT security measures are applied.
- **Severity** describes the potential adverse impact of a vulnerability being exploited

Source: GAO analysis of DLA and NIST information. | GAO-21-278.

- Additionally, DLA did not completely document security controls assessed as non-compliant in both the security assessment and risk assessment reports. Specifically, five of the six selected inventory management systems did not include key information, such as descriptions of issues, issue severity, recommendations, residual risk, threat, likelihood, potential impact, and mitigations. For example, a risk assessment report denoted a lack of data mining protection as one of the non-compliant controls.[32] However, DLA did not include proposed mitigations for addressing this non-compliant control.

  When we discussed this issue with DLA officials, they agreed with our analysis and told us that these specific risk attributes were not available to be populated in the eMASS system. The same officials have stated that the eMASS system was updated—in April 2018—to require these risk attributes, and that they are tracked quarterly. We acknowledge that DLA updated the eMASS system in April 2018 to include additional data fields; however, all six of the selected inventory management systems we reviewed were authorized subsequent to that update and did not include this information.

Key Concept

Inherited controls are controls in which one information system receives protection from security controls (or portions of security controls) that are developed, implemented, and assessed, authorized, and monitored by entities other than those responsible for the system or application.

Source: GAO analysis of DOD and Committee on National Security Systems information. | GAO-21-278

- Similarly, DLA program officials did not have certain information—such as severity and recommendations—for controls that were inherited from other DOD components. The officials stated that inherited controls are the responsibility of the entity providing the controls.[33] When we discussed this issue with DLA officials, they acknowledged the missing information. However, they told us that DLA is not responsible for and is unable to edit information provided for controls inherited from another DOD component. They stated that, as a result, DLA's authorizing officials considered the impact associated with the missing information to help inform system risk and the decision to authorize the system. Although inherited controls are

[32]Data mining is an analytical process that attempts to find correlations or patterns in large data sets for the purpose of data or knowledge discovery. Sensitive information can be extracted from data mining operations. Data mining prevention and detection techniques include limiting the number and frequency of database queries, limiting types of responses provided to database queries, and notifying personnel when atypical database queries or accesses occur.

[33]DLA inventory management systems meet some security control requirements through inherited controls, which are provided by the Defense Information Systems Agency, among others.

implemented by different DOD components, DLA remains responsible for ensuring that its authorizing officials receive complete information

for all controls, including inherited controls, before authorizing the system to operate.

- Further, the authorization packages did not include corrective action plans to address all weaknesses identified during the security control assessments for 29 non-compliant security controls, at least four of which were categorized as moderate-risk.[34] DLA officials stated that they believed corrective action plans had been created for all noncompliant security controls, and that the eMASS system would have prevented DLA officials from proceeding with their authorization process without corrective action plans for noncompliant controls.[35] Nevertheless, the authorization packages did not include corrective action plans to address 29 non-compliant controls.

DOD's risk management framework and DLA's related standard operating procedures require programs to obtain security authorization approval before systems become operational. When determining that a system should operate, the authorizing official issues a decision to formally accept the system's risk on behalf of the organization and the nation as a whole based on accurate and complete descriptions of security measures that have been implemented and corrective action plans for deficient/non-compliant controls.

To inform this decision, DLA's standard operating procedures require program officials to prepare a security authorization package that includes, among other things, a security assessment report, a risk assessment report, and corrective action plans. Both security assessment reports and risk assessment reports are to address the extent to which security controls complied with implementation requirements. Corrective action plans are required for all non-compliant security controls and should be maintained throughout a system's life cycle.[36] The corrective

[34]Four non-compliant controls were moderate-risk and 23 were low-risk. DLA did not identify the risk level for two of these non-compliant controls.

[35]DLA uses the Enterprise Mission Assurance Support Service, which is managed by the Defense Information Systems Agency, as its tool for supporting the implementation of risk management framework steps.

[36]DLA Standard Operating Procedure 8510.01-01.

action plans assist program officials in tracking progress toward addressing those weaknesses, among other things.

DLA's security authorization packages were not consistent and complete in that the agency had not established a process for program offices to review authorization documentation prior to submitting the package to the authorizing official. Having a process for reviewing security authorization packages for consistency and completeness would have provided an opportunity for DLA program officials to discover missing or inconsistent data, and to address these data flaws. According to DLA officials, security authorization packages are reviewed and submitted through the eMASS system. Although DLA updated its document approval process in the 2020 revisions to the DLA standard operating procedures, the agency did not address the issues identified above regarding consistent and complete compliance information.

Without a review of the consistency and completeness of the information provided in its authorization documentation—to include inherited controls and corrective action plans— DLA management may not have a full understanding of the nature of the cybersecurity risks it is accepting when authorizing a system to operate. Additionally, DLA may be at greater risk of unnecessarily exposing its inventory management programs to potential malicious or inadvertent exploitation from insider or other types of threats.

DLA Is Monitoring Security Controls, but Additional Actions Are Needed to Manage Ongoing Risk

DLA has undertaken some actions to monitor the security status of the six systems. For example, DLA established an agency-wide monitoring schedule for the annual assessment of implemented security controls. According to DLA documents, consistent with this schedule, the program offices generally conduct monthly security control assessments on a subset of security controls across all their systems, monitor the status of remedial actions, and brief management on security status. Additionally, as part of their continuous monitoring responsibilities, program offices have taken actions to remediate some deficiencies noted in their corrective action plans.

However, we identified three deficiencies that limit DLA's ability to effectively monitor and manage risk to the six systems we reviewed and other DOD systems that could be accessed if a malicious cyber actor compromised the six selected systems. Specifically,

- **Backlog in remediation of deficiencies:** DLA has not always remediated deficiencies identified in corrective action plans in a timely manner. Specifically, 1,115 of the 1,627 corrective action plans (69 percent) associated with the six inventory management systems exceeded the allowable amount of time for completion based on DLA standard operating procedures. These 1,115 corrective action plans were ongoing for an average of 485 days. DLA standard operating procedures require programs to conduct remediation identified in corrective action plans during continuous monitoring, and to complete their corrective action plans within a maximum of 365 days or fewer. DLA cybersecurity officials acknowledged a backlog in their remediation efforts.
- **Lack of waivers to continue to operate with deficiencies:** DLA's inventory management systems with security control deficiencies that exceed the deadline for being mitigated have not received waivers to continue to operate. For example, we found that 338 of the 1,115 corrective actions plans (30 percent) that exceeded the DLA standard operating procedure time threshold for completing corrective actions (which is driven by risk) required waivers to accept the continued risk to the system. However, DLA officials were unable to provide evidence that any of these corrective action plans had received a waiver.

  According to DLA standard operating procedures, when a program is unable to address deficiencies identified in a corrective action plan within twice the number of days allowed (as determined by its residual risk level), or within 365 days of the plan's creation date, the program must request and obtain a waiver accepting the continued risk to the system (referred to as "authorizing official risk acceptance") from the designated authorizing official. The waiver is intended to provide the program more time to complete the necessary corrective actions.

  According to DLA cybersecurity officials, the scheduled deadlines for corrective action plans were established with the April 2020 update of the DLA standard operating procedures. However, our review of the September 2018 DLA standard operating procedures—which were in effect when the systems we were reviewing were going through reauthorization—also included this time frame, as well as a waiver requirement for corrective action plans that exceeded their scheduled deadlines. Additionally, DLA officials stated that the agency had conducted a pilot program from May to July 2020 to automate the risk

acceptance process in the eMASS system that further delayed the approval of waiver requests until August 2020.

Until DLA's Cybersecurity Office completes its revisions and implements its waiver review and approval process for obtaining waivers that accept identified ongoing risk for the 338 corrective action plans awaiting waivers, DLA management will continue to be hampered in its monitoring and risk management activities by an incomplete understanding of the systems' risks.

- **Lack of key information in corrective action plans.** Corrective action plans that were developed to address security control deficiencies did not consistently contain key information. For example, DLA developed 1,627 corrective action plans to address security control deficiencies across the six inventory management systems. However, 27 of those did not consistently identify the residual risk level. Knowing the residual risk level is important because it would provide the authorizing official and the DLA program official with information to identify whether deficiencies are being addressed in a timely manner.

  Key information is missing because DLA program offices did not include required information in corrective action plans. DLA standard operating procedures require that deficiencies identified in a corrective action plan be addressed within a certain amount of time after the plan is created based on the residual risk level associated with the plan. For example, remediation actions in a plan with high residual risk are to be completed within 30 days, while remediation for a low residual risk plan is to be completed within 180 days. However, without having the residual risk level, DLA officials are unable to validate that the deficiencies identified in the 27 corrective action plans are remediated within those deadlines, and systems may be at increased risk of exploitation.

Key Concept

Within DLA, corrective action plans must be resolved within a specific time frame based on a security control's residual risk level. Specifically,

- High or very high risk corrective action plans cannot exceed 30 days
- Moderate risk corrective action plans cannot exceed 90 days
- Low risk corrective action plans cannot exceed 180 days; and
- Very low risk corrective action plans cannot exceed 365 days.

Source: GAO analysis of DLA information. | GAO-21-278

Conclusions

Given the increased risk of cyber-based intrusions and attacks on both federal and nonfederal systems, cybersecurity risk management is critical. DLA has taken steps to manage life-cycle cybersecurity risk by categorizing systems based on risk and establishing an approach to implement security controls for six selected systems. However, DLA has not consistently developed a monitoring strategy to assess these controls' effectiveness; did not approve its security assessment plans before the

assessments were conducted; has not always fully supported system authorization decisions; and has not undertaken key monitoring actions.

These deficiencies, if left unresolved, could impair DLA's ability to effectively manage cyber risks to the six systems we reviewed and potentially pose risks to other DOD systems that could be accessed if a malicious cyber actor compromised DLA's systems. Until DLA addresses the identified deficiencies, the six selected inventory management systems and their operations will remain at increased risk of exploitation.

Recommendations for Executive Action

We are making a total of five recommendations to the Secretary of Defense.

The Secretary of Defense should ensure that the Director of DLA revises its standard operating procedures to require program offices to develop a system-specific monitoring strategy that is consistent with DOD's risk management framework and related NIST guidance. (Recommendation 1)

The Secretary of Defense should ensure that the Director of DLA revises and implements an assessment plan approval process that ensures that a designated authorizing official reviews and approves system assessment plans prior to a system being assessed. (Recommendation 2)

The Secretary of Defense should ensure that the Director of DLA directs the DLA Cybersecurity Office to establish a process for program offices to review the consistency and completeness of authorization documentation prior to submitting the package to the designated authorizing officials. (Recommendation 3)

The Secretary of Defense should ensure that the Director of DLA revises and implements the agency's process for obtaining waivers that accept identified ongoing risk–including the 338 corrective action plans awaiting waivers. (Recommendation 4)

The Secretary of Defense should ensure that the Director of DLA includes required information—such as residual risk levels—in corrective action plans. (Recommendation 5)

Agency Comments and Our Evaluation

We provided a draft of this report to DOD for review and comment. In its written responses to our recommendations, reproduced in appendix II, DLA partially concurred with three and concurred with two of our recommendations.

DLA partially concurred with our first recommendation to revise its standard operating procedures to require program offices to develop a system-specific monitoring strategy that is consistent with DOD's risk management framework and related NIST guidance. In its written comments, DLA stated that the system-level continuous monitoring section of the implementation plan was not initially required by the Enterprise Mission Assurance Support Service (eMASS) system. Additionally, DLA disagreed that there are not monitoring strategies to determine the effectiveness of security controls. DLA stated its Enterprise Continuous Monitoring Schedule outlines a two-year schedule to monitor the effectiveness of security controls for each DLA information system. According to DLA, this schedule includes a requirement to assess the security controls and document test results on a monthly basis in eMASS.

Although DLA asserts that eMASS did not initially require a system-level continuous monitoring section the DOD risk management framework stated that such plans should exist. As noted previously in this report, the DOD risk management framework in effect when these six systems went through authorization required a separate continuous monitoring strategy for each system. While DLA developed an agency-wide monitoring schedule for annual assessments of security controls, the monitoring strategies for three systems did not fully meet DOD requirements and related NIST guidance because they did not sufficiently describe how the effectiveness of security controls would be monitored on a continual basis. Further, DLA did not develop monitoring strategies for the other three systems. We noted that DLA's current standard operating procedures for cybersecurity, which emphasize an enterprise-wide monitoring strategy in the absence of system-level monitoring strategies, conflict with the requirements and intent of DOD's risk management framework and NIST recommendations for such strategies.

DLA stated that the agency plans to update its Risk Management Framework Standard Operating Procedure by December 31, 2021, to require a system-level continuous monitoring strategy that documents any monitoring efforts in addition to the DLA Enterprise Continuous Monitoring

Schedule. We believe this update could address DOD requirements and related NIST guidance. It will be important for the strategy developed under the new standard operating procedure to include elements that call for defining the ongoing control assessment approach and describing how ongoing assessments are to be conducted. Such details are important for ensuring that the effectiveness of a system's controls are monitored through appropriate methods and with a level of rigor commensurate with the system's risk.

DLA partially concurred with our second recommendation to revise and implement an assessment plan approval process that ensures a designated authorizing official reviews and approves the system assessment plans prior to the system being assessed. In its written comments, DLA stated that assessment plans were not approved by the authorizing official prior to the assessment and validation activities because, while transitioning to the DOD risk management framework, DLA chose to take a more streamlined approach of approving assessment plans during the initial authorization issuance. However, as we noted in the report DLA's approach was inconsistent with the requirements in DOD's risk management framework. DLA agreed that there were missed opportunities for risk-based decisions because of the approach that it took.

DLA stated that the agency plans to update its standard operating procedure by May 1, 2022, to require the security plan—which contains the assessment plan—be approved prior to any assessment or validation activities. DLA stated that the agency plans to utilize an eMASS workflow to ensure the authorizing official or their representative approves the security plan. If implemented as described, the actions that DLA plans to take in response to this recommendation should address the weaknesses we identified. As discussed earlier in the report, reviewing and approving the assessment plan prior to conducting the assessment will ensure that DLA's planning efforts are sufficient and that its inventory management systems are appropriately assessed.

DLA partially concurred with our third recommendation to establish a process for program offices to review the consistency and completeness of authorization documentation prior to submitting the package to the designated authorizing officials. In its written comments, DLA stated that missing items identified during the audit have been added to the corrective action plans in eMASS, and that the agency has a robust approval process for corrective action plans to ensure items are completed properly and thoroughly. For example, DLA stated that eMASS

has made corrective action elements required fields that must be filled out when new plans are created. Additionally, the agency stated they have ensured all existing corrective action plans have required fields populated and provided documentation to demonstrate such actions.

DLA provided us a spreadsheet that was to demonstrate those fields we found incomplete during our review have since been completed. By adding the risk level to each deficiency, authorizing officials will be in a position to make more risk-informed decisions. For example, this information could help them prioritize mitigations and responses to threats. However, the agency did not provide evidence demonstrating the existence or improvement of a process to review authorization documentation (i.e. a process that would or should have caught these missing fields prior to our audit). As previously stated, having a process for reviewing security authorization packages for consistency and completeness could provide an opportunity for DLA program officials to discover missing or inconsistent data, and to address these data flaws. Until DLA has such a process in place these issues could resurface in reviews of these and other systems.

DLA concurred with our fourth recommendation to revise and implement the agency's process for obtaining waivers that accept identified ongoing risk-including the 338 corrective action plans awaiting waivers. In its written comments, DLA acknowledged that the approval timeline for its risk waivers were a root cause for the backlog in their remediation of deficiencies. DLA stated that it has successfully implemented an approval process for obtaining waivers. Further, DLA stated that it believes that its implemented actions fully address the recommendation. However, DLA did not provide evidence that the agency has implemented an approval process for obtaining waivers that accept identified ongoing risk for the 338 and any subsequent corrective action plans awaiting waivers. The implementation of a revised process could improve DLA's ability to effectively monitor and manage risk to the six systems we reviewed and other DOD systems that could be accessed through the six selected systems. We will continue to monitor the agency's efforts in implementing our recommendation.

DLA concurred with our fifth recommendation to ensure the Director of DLA include required information in correction active plans—such as residual risk levels. In its written comments, DLA acknowledged some missing risk information for the six inventory management systems reviewed. DLA stated it has ensured all existing ongoing corrective actions have complete information and provided supporting

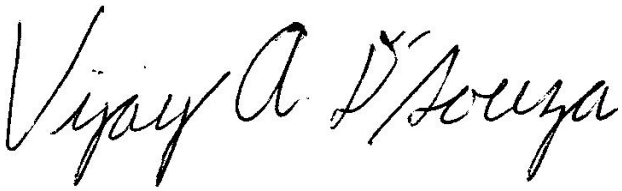
documentation as evidence of these actions. Additionally, DLA stated that it believes it has a robust approval process that ensures all elements of the corrective action plans are completed properly and thoroughly.

However, DLA did not provide us evidence that the agency had revised its approval process for corrective actions plans to address the underlying issues we identified. Consequently, these issues could resurface in future reviews of these and other systems. As previously mentioned in this report, knowing the residual risk level could provide the authorizing official and DLA program official's information to identify whether deficiencies are being addressed in a timely manner. We will continue to monitor the agency's progress in implementing our recommendation.

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

If you or your staff have any questions about this report, please contact us at (202) 512-9627 or maurerd@gao.gov or at (202) 512-6240 or dsouzav@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 contributions to this report are listed in appendix III.

Diana Maurer
Director, Defense Capabilities and Management



Vijay A. D'Souza
Director, Information Technology and Cybersecurity

Appendix I: Objective, Scope, and Methodology

The objective of our review was to determine the extent to which DLA has implemented key risk management steps to address cybersecurity risks to its inventory management systems.

To address our objective, we interviewed Defense Logistics Agency (DLA) cybersecurity officials to identify the systems they deemed critical to their inventory management operations, including those that interface with contractors and commercial networks. Based on those interviews and on our review of DLA documents, we selected six systems to examine in this review. Among the ten systems DLA identified, these six were independent inventory management systems rather than modules of broader systems.

To determine the extent to which DLA undertook risk management steps to address cybersecurity risks to its inventory management systems, we reviewed Department of Defense (DOD) and DLA cybersecurity guidance and DLA's authorization documentation for the six selected inventory management systems. The six selected systems were authorized between May 2018 and November 2019 and were the most recent authorizations to operate in September 2019. We evaluated the documentation against the six risk management steps identified in DOD's Instruction on cybersecurity risk management (also referred to as the DOD risk management framework).[1] This framework identifies six key risk management steps (each of which includes several tasks that must be performed), listed below, that are applicable to individual systems:

1. categorize the system,
2. select security controls,
3. implement security controls,

[1]DOD Instruction 8510.01, *Risk Management Framework (RMF) for DOD Information Technology (IT)*, (March 12, 2014) (incorporating Change 2, July 28, 2017). DOD updated this Instruction in December 2020 but did not include any substantive changes to the steps that we evaluated at the system level. We did not use the updated version of this guidance in our review, as we focused on the agency's risk management framework actions from the 2018 and 2019 system authorizations, as noted earlier.

4. assess security controls,
5. authorize the system, and
6. monitor security controls.

While we primarily evaluated DLA's efforts against guidance in DOD's Instruction on cybersecurity risk management, we also evaluated DLA's efforts against certain guidance identified in the National Institute of Standards and Technology's (NIST)[2] and from the Committee on National Security Systems Instruction (CNSSI) No. 1253,[3] because DOD's Instruction directs DLA to also comply with these documents. We also reviewed requirements from DLA's standard operating procedures for implementing the risk management framework.[4] To better understand DOD's risk management framework, we interviewed officials from DOD's Office of the Chief Information Officer and Office of the Deputy Chief Management Officer.

To determine the extent to which DLA has implemented risk management steps to address cybersecurity risks to its inventory management systems, we obtained and analyzed documents used by DLA cybersecurity officials to implement, oversee, and demonstrate compliance with risk management steps. Specifically, we reviewed the system categorization results, system security plans, security assessment reports, authorizations to operate documentation, corrective action plans, and system-level continuous monitoring strategies, where available. We also reviewed timeliness and risk data from DOD's IT tool for managing the risk management framework to assess the six DLA program offices' efforts to implement these risk management steps. We evaluated these documents and data against requirements from the six risk management

[2]NIST Special Publication 800-53A, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*, Revision 4 (December 2014).

[3]Although the six systems in this report are critical to DLA operations, these systems are not national security systems. 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 (CNSSI) No. 1253. This guidance builds on and is a companion document to NIST guidance relevant to categorization and selection.

[4]Defense Logistics Agency, Standard Operating Procedure 8510.01-01, *DLA Risk Management Framework*, Sep 25, 2018. DLA updated this standard operating procedure in April 2020. We did not use the updated version of this guidance in our review, as we focused on the agency's risk management framework actions from the 2018 and 2019 system authorizations, as noted earlier.

steps identified in DOD's risk management framework and supplemental risk guidance, as well as DLA's related standard operating procedures.[5] We supplemented our analysis of documents and data by interviewing officials in DLA's Cybersecurity Office and the system program offices about their efforts to assess, document, and review security controls for their respective systems. We then made determinations about the extent to which each system's program office had fully addressed, partially addressed, or not addressed all aspects of the required tasks for the risk management step based on the documents and data provided.

In reviewing each of the six risk management steps, we used professional judgment to identify a subset of the activities that we believed would sufficiently characterize DLA's implementation of the risk management framework. In doing so, we excluded one of the three required activities associated with the implementation step. Specifically, in DOD's risk management framework, the third step is to "implement security controls." This step identifies three activities: (1) implement the security controls specified in the security plan in accordance with DOD implementation guidance, (2) document the security control implementation in the security plan, and (3) identify security controls that are available for inheritance by other systems and their associated compliance status from the hosting or connected systems.

We assessed the extent to which each system's program office addressed this step based on whether the office documented its approach to implement the selected security controls and identified inherited controls for each of the six inventory management systems. We did not verify or assess program offices' implementation of security controls due to the significant investment in time and resources required to do so, given the large volume of data and variety of system-specific implementation approaches across the six systems. For reporting purposes and consistency with the aspects that we evaluated, we refer to this step as "establish implementation approach" in this report.

DLA provided documentation to support the most recent authorizations to operate at the time we began our review in September 2019. In addition, DLA provided timeliness and risk data for corrective action plans to

[5]DOD Instruction 8510.01. DOD, *Program Managers Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle*, (September 2015 Version 1). DLA, *Standard Operating Procedure*, 8510.01-01 (Sep. 25, 2018)

address identified vulnerabilities for each system from March 2020, and ongoing assessment data related to continuous monitoring activities.[6] Much of this information was obtained from DOD's IT tool for managing the risk management framework—eMASS—that supports the collection, review, and approval of information regarding systems' completion of steps in DOD's risk management framework.[7] To better understand how eMASS supports DLA, we observed demonstrations of how DLA used this tool to perform risk management framework steps.

To assess the reliability of data obtained from eMASS, we interviewed knowledgeable officials in the agency's Cybersecurity Office and the selected systems' program offices about the quality control procedures used to ensure the accuracy and completeness of the data. We also compared the data to other relevant documentation on each system's security controls. We found that most of the security controls data we examined were sufficiently reliable for evaluating DLA's risk management steps for the selected inventory management systems. We noted in our report where discrepancies in the data impacted the system program offices' ability to address DOD's risk management steps.

This report does not address the extent to which DLA and the selected systems' countermeasures are able to successfully prevent certain cyberattacks. Rather, it focuses on DLA's efforts to manage the cybersecurity of these six systems through a risk management framework that is intended to help managers make informed decisions about cyber threats, and to prioritize mitigations and responses to threats in the most cost-effective manner.

We have included key concept boxes throughout the report to assist the reader's understanding of cybersecurity terminology. These concepts are not formal definitions of these terms but are based on our analysis of

[6]DOD and NIST documents refer to this information as plans of actions and milestones. We refer to the DOD plans of actions and milestones as "corrective action plans" throughout this report.

[7]DLA uses the Enterprise Mission Assurance Support Service, which is managed by the Defense Information Systems Agency, as its tool to support its implementation of risk management framework steps.

various publications from CNSS, DOD, and DLA, and NIST publications.[8] DOD uses various sources to define its cybersecurity terms, including CNSS and NIST publications.[9]

We conducted this performance audit from September 2019 to June 2021 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.

[8]For example, National Institute of Standards and Technology (NIST), *Risk Management Framework for Information Systems and Organizations,* Special Publication 800-37, Revision 2 (Gaithersburg, Md.: December 2018); Committee on National Security Systems Instruction (CNSSI) No. 1253, *Security Categorization and Control Selection for National Security Systems* (Mar. 27, 2014); DOD Instruction 8510.01; DOD, *Program Managers Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle*, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (September 2015 Version 1); and Defense Logistics Agency, Standard Operating Procedure, 8510.01-01, *DLA Risk Management Framework (RMF)* (Sept. 25, 2018).

[9]For example. National Institute of Standards and Technology (NIST), Glossary, May 2021, https://csrc.nist.gov/glossary; and Committee on National Security Systems Instruction (CNSSI) No. 4009, *Committee on National Security Systems (CNSS) Glossary* (April 6, 2015). For a more complete list of cybersecurity terms, see DOD 8510.01.

Appendix II: Comments from the Defense Logistics Agency

DEFENSE LOGISTICS AGENCY
HEADQUARTERS
8725 JOHN J. KINGMAN ROAD
FORT BELVOIR, VIRGINIA 22060-6221

19 MAY 2021

Ms. Diana Maurer
Director, Defense Capabilities Management
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Ms. Maurer:

This is the Department of Defense (DoD) response to the Government Accountability Office (GAO) Draft Report GAO-21-278, "DEFENSE CYBERSECURITY: Defense Logistics Agency Needs to Address Risk Management Deficiencies in Inventory Systems," dated April 21, 2021 (GAO Code 103814). Detailed comments on the report recommendations are enclosed.

The point of contact (POC) for this effort is Mr. Andy Hagenow at 571-767-6204, or email: andrew.hagenow@dla.mil.

Sincerely,

DUCHAK.GEORGE.D.1086741578 Digitally signed by DUCHAK.GEORGE.D.1086741578 Date: 2021.05.19 12:35:19 -04'00'

GEORGE D. DUCHAK, PhD, PE
Director, DLA Information Operations
Chief Information Officer

Enclosure:
As stated

SUBJECT: DoD Response to Draft Report for Audit of DEFENSE CYBERSECURITY: Defense Logistics Agency Needs to Address Risk Management Deficiencies in Inventory Management Systems (Project #103814; Report GAO-21-278)

RECOMMENDATION 1: The Secretary of Defense should ensure that the Director of DLA revises its standard operating procedures to require program offices to develop a system-specific monitoring strategy that is consistent with DoD's risk management framework and related NIST guidance.

DoD Comments: Partially Concur.
While the System Level Continuous Monitoring section of the Implementation Plan within eMASS was not completely filled out for all the applicable inventory management systems, the incomplete fields were not required when initially added to the Implementation Plan in Enterprise Mission Assurance Support Service (eMASS). Further, DLA does not agree that there are not monitoring strategies to determine the effectiveness of security controls. As mentioned by the GAO, the DLA Enterprise Continuous Monitoring Schedule outlines a two-year schedule to monitor the effectiveness of security controls for each DLA information system. The system is required to assess the security controls and document through Test Results on a monthly basis entered in eMASS. The effectiveness and compliance of each assessment procedure contained within every security control in their security control baseline is assessed by the ISSM and validated by the SCA Representative team. To fully address this recommendation, DLA will update the DLA Risk Management Framework Standard Operating Procedure (DLA RMF SOP) to explicitly require each system to document their system level continuous monitoring strategy as a part of the Implementation Plan in eMASS. This system level continuous monitoring strategy would document any system level monitoring in addition to the DLA Enterprise Continuous Monitoring Schedule. The expected completion date for this action is December 31, 2021.

RECOMMENDATION 2: The Secretary of Defense should ensure that the Director of DLA revises and implements an assessment plan approval process that ensures a designated authorizing official reviews and approves the system assessment plans prior to the system being assessed.

DoD Comments: Partially Concur.
Assessment plans were not approved by the Authorizing Official prior to the assessment and validation activities being performed because, while transitioning to RMF, DLA chose to take a more streamlined approach of approving assessment plans during the initial authorization issuance. DLA does agree that there were missed opportunities for risk-based decisions. Any missing information or discrepancies identified with the contents of the authorization request, to include the assessment plans, were identified as terms and conditions in the initial authorization issuances. Additionally, all authorization issuances were based on the risk posture as documented in eMASS, to include risk identified in Non-Compliant security controls and the

associated POA&M items. (DLA uses eMASS, which automatically assigns the appropriate DoD assessment procedures applicable to the system based on system security categorization.) To more fully address the recommendation, DLA will update the DLA RMF SOP to require the Security Plan (which contains the assessment plan) be approved prior to any assessment or validation activities being performed. DLA will utilize the Security Plan Approval workflow in eMASS to ensure the Authorizing Official or Authorizing Official Designated Representative approve the Security Plan. The expected completion date for this action is May 1, 2022.

RECOMMENDATION 3: The Secretary of Defense should ensure that the Director of DLA directs the DLA Cybersecurity office to establish a process for program offices to review the consistency and completeness of authorization documentation prior to submitting the package to the designated authorizing officials.

DoD Comments: Partially Concur.
Missing items identified during the audit have been added to the Plan of Action and Milestones (POA&M) items in eMASS and systems are required to go back and populate them for all existing POA&M items for both POA&Ms created by DLA and those passed down through inheritance from external systems. DLA does not agree that there is no established process to review authorization documentation prior to submitting an authorization request. DLA has established a robust POA&M approval process which requires every system to submit new POA&M items for approval on a quarterly basis. Part of that approval is to ensure all elements of the POA&M items are completed properly and thoroughly. In cases where the POA&M item is owned by an external system, the POA&M is reviewed for completeness and the PM and ISSM are required to work with the POA&M owner to ensure any POA&M discrepancies are addressed by the POA&M owner. Additionally, eMASS has made those POA&M elements required fields that must be filled out when creating new POA&M items, and DLA has also ensured that all existing DLA owned ongoing POA&M items have these POA&M fields populated. DLA believes that the implemented actions fully address the recommendation and requests closure.

RECOMMENDATION 4: The Secretary of Defense should ensure that the Director of DLA revises and implements the agency's process for obtaining waivers that accept identified ongoing risk-including the 338 corrective action plans awaiting waivers.

DoD Comments: Concur.
A backlog of Authorizing Official approval for waivers (which DoD refers to as Authorizing Official Risk Acceptance (AORA)) resulted in corrective action plans (POA&M items) not always being completed within the maximum duration allowed in the DLA RMF SOP. The approval timeline for granting an AORA had already been identified as the root cause for the backlog prior to the GAO review. DLA has successfully implemented the AORA and Aged POA&M processes in eMASS. The AORA process has reduced the approval timeline from

eight months to 60 days. Additionally, aged POA&M items that are ongoing for more than 365 days, additional documentation from the Program Manager and in some cases the Portfolio Manager is required to be provided in the approval request. This ensures additional management visibility and ownership in closing out the ongoing POA&M items. DLA believes that the implemented actions fully address the recommendation and requests closure.

RECOMMENDATION 5: The Secretary of Defense should ensure that the Director of DLA includes required information in corrective action plans-such as residual risk levels.

DoD Comments: Concur.
DLA concurs that residual risk was missing for some of the six inventory management systems reviewed. DLA has established a robust POA&M approval process which requires every system to submit new POA&M items for approval on a quarterly basis. Part of that approval is to ensure all elements of the POA&M items are completed properly and thoroughly. In cases where the POA&M item is owned by an external system, the POA&M is reviewed for completeness and the PM and ISSM are required to work with the POA&M owner to ensure any POA&M discrepancies are addressed by them. Additionally, eMASS has made those POA&M elements required fields that must be filled out when creating new POA&M items. DLA has also ensured that all existing DLA owned ongoing POA&M items have these POA&M fields populated. DLA believes that the implemented actions fully address the recommendation and requests closure.

Text of Appendix II: Comments from the Defense Logistics Agency

Page 1

19 MAY 2021

Ms. Diana Maurer

Director, Defense Capabilities Management

U.S. Government Accountability Office 441 G Street, N.W.

Washington, DC 20548

Dear Ms. Maurer:

This is the Department of Defense (DoD) response to the Government Accountability Office (GAO) Draft Report GAO-21-278, “DEFENSE CYBERSECURITY: Defense Logistics Agency Needs to Address Risk Management Deficiencies in Inventory Systems,” dated April 21, 2021 (GAO Code 103814). Detailed comments on the report recommendations are enclosed.

The point of contact (POC) for this effort is Mr. Andy Hagenow at 571-767-6204, or email: andrew.hagenow@dla.mil.

Sincerely,

GEORGE D. DUCHAK, PhD, PE

Director, DLA Information Operations Chief Information Officer

Enclosure:

As stated

Page 2

SUBJECT: DoD Response to Draft Report for Audit of DEFENSE CYBERSECURITY: Defense Logistics Agency Needs to Address Risk

Management Deficiencies in Inventory Management Systems (Project #103814; Report GAO-21-278)

RECOMMENDATION 1: The Secretary of Defense should ensure that the Director of DLA revises its standard operating procedures to require program offices to develop a system-specific monitoring strategy that is consistent with DoD's risk management framework and related NIST guidance.

DoD Comments: Partially Concur.

While the System Level Continuous Monitoring section of the Implementation Plan within eMASS was not completely filled out for all the applicable inventory management systems, the incomplete fields were not required when initially added to the Implementation Plan in Enterprise Mission Assurance Support Service (eMASS). Further, DLA does not agree that there are not monitoring strategies to determine the effectiveness of security controls. As mentioned by the GAO, the DLA Enterprise Continuous Monitoring Schedule outlines a two- year schedule to monitor the effectiveness of security controls for each DLA information system. The system is required to assess the security controls and document through Test Results on a monthly basis entered in eMASS. The effectiveness and compliance of each assessment procedure contained within every security control in their security control baseline is assessed by the ISSM and validated by the SCA Representative team. To fully address this recommendation, DLA will update the DLA Risk Management Framework Standard Operating Procedure (DLA RMF SOP) to explicitly require each system to document their system level continuous monitoring strategy as a part of the Implementation Plan in eMASS. This system level continuous monitoring strategy would document any system level monitoring in addition to the DLA Enterprise Continuous Monitoring Schedule. The expected completion date for this action is December 31, 2021.

RECOMMENDATION 2: The Secretary of Defense should ensure that the Director of DLA revises and implements an assessment plan approval process that ensures a designated authorizing official reviews and approves the system assessment plans prior to the system being assessed.

DoD Comments: Partially Concur.

Assessment plans were not approved by the Authorizing Official prior to the assessment and validation activities being performed because, while transitioning to RMF, DLA chose to take a more streamlined approach of approving assessment plans during the initial authorization issuance. DLA does agree that there were missed opportunities for risk-based decisions. Any missing information or discrepancies identified with the contents of the authorization request, to include the

assessment plans, were identified as terms and conditions in the initial authorization issuances. Additionally, all authorization issuances were based on the risk posture as documented in eMASS, to include risk identified in Non-Compliant security controls and the

associated POA&M items. (DLA uses eMASS, which automatically assigns the appropriate DoD assessment procedures applicable to the system based on system security categorization.) To more fully address the recommendation, DLA will update the DLA RMF SOP to require the Security Plan (which contains the assessment plan) be approved prior to any assessment or validation activities being performed. DLA will utilize the Security Plan Approval workflow in eMASS to ensure the Authorizing Official or Authorizing Official Designated Representative approve the Security Plan. The expected completion date for this action is May 1, 2022.

RECOMMENDATION 3: The Secretary of Defense should ensure that the Director of DLA directs the DLA Cybersecurity office to establish a process for program offices to review the consistency and completeness of authorization documentation prior to submitting the package to the designated authorizing officials.

DoD Comments: Partially Concur.

Missing items identified during the audit have been added to the Plan of Action and Milestones (POA&M) items in eMASS and systems are required to go back and populate them for all existing POA&M items for both POA&Ms created by DLA and those passed down through inheritance from external systems. DLA does not agree that there is no established process to review authorization documentation prior to submitting an authorization request. DLA has established a robust POA&M approval process which requires every system to submit new POA&M items for approval on a quarterly basis. Part of that approval is to ensure all elements of the POA&M items are completed properly and thoroughly. In cases where the POA&M item is owned by an external system, the POA&M is reviewed for completeness and the PM and ISSM are required to work with the POA&M owner to ensure any POA&M discrepancies are addressed by the POA&M owner. Additionally, eMASS has made those POA&M elements required fields that must be filled out when creating new POA&M items, and DLA has also ensured that all existing DLA owned ongoing POA&M items have these POA&M fields populated. DLA believes that the implemented actions fully address the recommendation and requests closure.

RECOMMENDATION 4: The Secretary of Defense should ensure that the Director of DLA revises and implements the agency's process for obtaining

waivers that accept identified ongoing risk-including the 338 corrective action plans awaiting waivers.

DoD Comments: Concur.

A backlog of Authorizing Official approval for waivers (which DoD refers to as Authorizing Official Risk Acceptance (AORA)) resulted in corrective action plans (POA&M items) not always being completed within the maximum duration allowed in the DLA RMF SOP. The approval timeline for granting an AORA had already been identified as the root cause for the backlog prior to the GAO review. DLA has successfully implemented the AORA and Aged POA&M processes in eMASS. The AORA process has reduced the approval timeline from

eight months to 60 days. Additionally, aged POA&M items that are ongoing for more than 365 days, additional documentation from the Program Manager and in some cases the Portfolio Manager is required to be provided in the approval request. This ensures additional management visibility and ownership in closing out the ongoing POA&M items. DLA believes that the implemented actions fully address the recommendation and requests closure.

RECOMMENDATION 5: The Secretary of Defense should ensure that the Director of DLA includes required information in corrective action plans-such as residual risk levels.

DoD Comments: Concur.

DLA concurs that residual risk was missing for some of the six inventory management systems reviewed. DLA has established a robust POA&M approval process which requires every system to submit new POA&M items for approval on a quarterly basis. Part of that approval is to ensure all elements of the POA&M items are completed properly and thoroughly. In cases where the POA&M item is owned by an external system, the POA&M is reviewed for completeness and the PM and ISSM are required to work with the POA&M owner to ensure any POA&M discrepancies are addressed by them. Additionally, eMASS has made those POA&M elements required fields that must be filled out when creating new POA&M items. DLA has also ensured that all existing DLA owned ongoing POA&M items have these POA&M fields populated.

DLA believes that the implemented actions fully address the recommendation and requests closure.

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Diana Maurer at (202) 512-9627 or maurerd@gao.gov

Vijay A. D'Souza at (202) 512-6240 or at dsouzav@gao.gov

Staff Acknowledgments

In addition to the contacts named above, Tommy Baril (Assistant Director), Josh Leiling (Assistant Director), Marilyn Wasleski (Assistant Director, retired), Ashley Houston (Analyst in Charge), Lamis Alabed, Wayne Emilien, Torrey Hardee, Katherine Noble, and Ed Yuen made key contributions to this report. Tracy Barnes, Rebecca Eyler, Christopher Gezon, Amie Lesser, Walter Vance, and Cheryl Weissman 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

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

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

Strategic Planning and External Liaison

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