United States Government Accountability Office

Report to Congressional Requesters

August 2023

DHS ACQUISITIONS

Opportunities Exist to Enhance Risk Management

GAO-23-106249

August 2023

DHS ACQUISITIONS

Opportunities Exist to Enhance Risk Management

GAO Highlights

Highlights of GAO-23-106249, a report to congressional requesters

Why GAO Did This Study

DHS and its components acquire systems to help carry out multiple critical missions. In fiscal year 2023, DHS plans to spend over $4 billion on these systems. In May 2019, DHS revised its acquisition policy to better incorporate risk management—a continuous process to systematically track and manage risks.

GAO was asked to review DHS's acquisition risk management process for its major acquisition programs—those with life-cycle cost estimates of $300 million or more. This report assesses, among other issues, the extent to which DHS has addressed risk management at (1) the program-level, including involving stakeholders and leadership, and (2) the portfolio level.

GAO reviewed acquisition risk management policies and guidance from DHS and the eight components that manage major acquisition programs. GAO also reviewed how a nongeneralizable sample of five programs from within these components managed risks. GAO selected the sample based on a representation of components and a mix of IT and non-IT programs, among other criteria.

What GAO Recommends

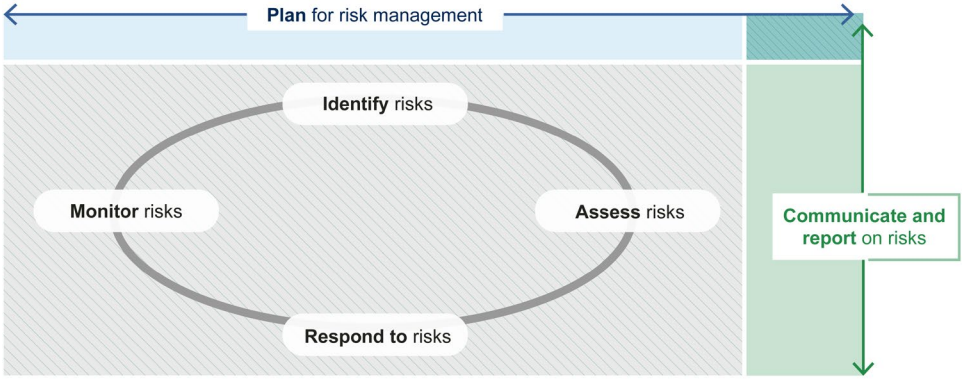
GAO is making eight recommendations to DHS, including that, as it updates its risk management guidance, it includes steps to enhance programs' communication with stakeholders, improve direction to programs on providing current risk data to leadership, and address portfolio risk management. DHS agreed with the recommendations.

View GAO-23-106249. For more information, contact Marie A. Mak at (202) 512-4841 or makm@gao.gov.

What GAO Found

Managing acquisition risks—potential negative effects on a program's cost, schedule, and performance—is critical for a program to achieve its objectives. GAO previously found that acquisition programs tend to be overly optimistic when assessing their risks, underestimating the resources or time needed to develop and field capabilities. GAO and others identified six leading principles of acquisition risk management that are applicable to programs and portfolios, which are groups of related programs, such as Coast Guard ships.

Leading Principles for Acquisition Risk Management Applicable to Programs and Portfolios



Source: GAO analysis of GAO and Project Management Institute, Inc. information. | GAO-23-106249

At the program level, the Department of Homeland Security's (DHS) risk management guidance broadly reflects these leading principles. DHS guidance encourages programs to engage with stakeholders and leadership throughout their acquisition life cycles. GAO found examples of this communication in practice, such as when programs prepared for acquisition decision events, a series of critical milestones designed for oversight. However, GAO found gaps in DHS guidance and programs' implementation of the communication leading principle. Specifically, GAO found instances in which selected programs did not consistently track and incorporate stakeholder input or provide current risk data to DHS leadership. Ensuring that DHS guidance conforms with leading principles on documenting stakeholder input and communicating up-to-date information to leadership would improve DHS's ability to manage acquisition risks.

DHS's guidance also falls short in addressing leading principles at the portfolio level, which involves consideration of interdependencies and enterprise-level risks. For example, the guidance does not address how officials should identify portfolio-level risks—one of the six leading principles. Further, officials from two DHS components stated that having portfolio risk management guidance would be helpful to ensure consideration of these risks. Having such guidance would enhance DHS's ability to manage risks across its portfolio of programs and make decisions that optimize the portfolio's resources rather than considering risks solely on a program-by-program basis. DHS plans to update its acquisition risk management guidance by fall of 2023, which presents an opportunity to address these gaps and enhance DHS's risk management process.

Contents

Letter		1
	Background	5
	DHS Addresses Leading Principles of Acquisition Risk Management but Lacks Guidance on Some Key Practices	12
	DHS Has Not Weighed Costs and Benefits of Implementing a Tool to Facilitate Risk Knowledge-Sharing	21
	Selected Programs Engage with Stakeholders and Leadership on Risk Management but Do Not Consistently Document This Involvement	25
	Conclusions	35
	Recommendations for Executive Action	36
	Agency Comments	38
Appendix I	Objectives, Scope, and Methodology	39
Appendix II	Summary of Department of Homeland Security Components' Risk Management Guidance	46
Appendix III	Comments from the Department of Homeland Security	47
Appendix IV	GAO Contact and Staff Acknowledgments	50

Tables

	Table 1: Leading Acquisition Risk Management Principles and Corresponding Instructions in DHS Guidance	12
	Table 2: Examples of Risk Tracking Tools by DHS Component	23
	Table 3: Selected DHS Major Acquisition Programs	43
	Table 4: Acquisition Risk Management Guidance of Department of Homeland Security (DHS) Components	46

Figures

	Figure 1: DHS Acquisition Decision Events in the Obtain Phase for Major Acquisition Programs	5

Figure 2: Leading Principles for Acquisition Risk Management 8
Figure 3: Notional Depiction of How DHS's Acquisition Portfolios Exist at Multiple Levels 11
Figure 4: Examples of Required Program Documents with Risk Information that DHS Leadership and Stakeholders Review throughout the Acquisition Life Cycle 26
Figure 5: Lag Time in a Selected Coast Guard Program's Risks Presented to Department of Homeland Security Leadership 34

Abbreviations

CBP	U.S. Customs and Border Protection
DHS	Department of Homeland Security
FEMA	Federal Emergency Management Agency
IT	information technology
PARM	Office of Program Accountability and Risk Management
PMBOK	Project Management Body of Knowledge
TSA	Transportation Security Administration

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

August 24, 2023

The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

The Honorable J. Luis Correa
Ranking Member
Subcommittee on Border Security and Enforcement
Committee on Homeland Security
House of Representatives

The Honorable Glenn Ivey
Ranking Member
Subcommittee on Oversight, Investigations and Accountability
Committee on Homeland Security
House of Representatives

Each year, the Department of Homeland Security (DHS) invests billions of dollars in a diverse portfolio of major acquisition programs to help execute its many critical missions. For example, DHS and its components are acquiring systems to help secure the border, screen travelers, enhance emergency communications, improve disaster response, and carry out other operations. Most of these programs have an estimated life-cycle cost of $300 million or more.[1] In fiscal year 2023, DHS plans to spend over $4 billion on these acquisition programs and more than $191 billion over the life cycle of these programs.

Managing acquisition risks—potential negative effects on a program's cost, schedule, and performance relative to its plan—is critical for a program to achieve its objectives. However, we previously found that acquisition programs tend to be overly optimistic when assessing their risks, underestimating the resources or time needed to develop and field

[1]DHS defines major acquisition programs as those with life-cycle cost estimates of $300 million or more. In some cases, DHS may define a program with a life-cycle cost estimate less than $300 million as a major acquisition if it has significant strategic or policy implications for homeland security, among other things.

capabilities.[2] As a result, programs cost more than initially promised and operators make do with aging assets and systems when new capabilities are delivered late. One way that programs can mitigate against the consequences of optimistic biases is to implement acquisition risk management—a continuous process with specific steps aimed at systematically tracking and managing risks. Acquisition risk management applies to both programs and portfolios. A portfolio is a group of related acquisition programs that contribute to a collective whole, such as the Coast Guard's portfolio of ship programs that contribute to its surface capability. In May 2019, DHS revised its acquisition policy to better reflect certain risk management practices.[3]

You asked us to review DHS's acquisition risk management process for its major acquisition programs. This report assesses the extent to which: (1) DHS has addressed acquisition risk management principles at the program and portfolio levels, (2) DHS has shared information to facilitate acquisition risk management, and (3) DHS has involved stakeholders and leadership in acquisition risk management.

To conduct our work, we reviewed acquisition risk management policies and guidance from DHS's Office of Program Accountability and Risk Management (PARM)—the office responsible for DHS's overall acquisition governance process. We selected a nongeneralizable sample of five major acquisition programs to include in our review based on a variety of criteria, such as program type and component. We selected one program from each of the following components:

- **Cybersecurity and Infrastructure Security Agency**: Next Generation Network Priority Services Phase 2,
- **Federal Emergency Management Agency (FEMA)**: Grants Management Modernization,

[2]GAO, *Coast Guard Acquisitions: Opportunities Exist to Reduce Risk for the Offshore Patrol Cutter Program,* GAO-21-9 (Washington, D.C.: Oct. 28, 2020); *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Program Costs,* GAO-20-195G (Washington, D.C.: Mar. 12, 2020); *Technology Readiness Assessment Guide: Best Practices for Evaluating the Readiness of Technology for Use in Acquisition Programs and Projects,* GAO-20-48G (Washington, D.C.: Jan. 7, 2020); and *Coast Guard Acquisitions: Polar Icebreaker Program Needs to Address Risks before Committing Resources,* GAO-18-600 (Washington, D.C.: Sept. 4, 2018).

[3]DHS Instruction 102-01-001, Revision 01, *Acquisition Management* (Mar. 9, 2016) (incorporating change 1, May 3, 2019).

- **Transportation Security Administration (TSA)**: Credential Authentication Technology,
- **U.S. Coast Guard:** Polar Security Cutter, and
- **U.S. Customs and Border Protection (CBP)**: Non-Intrusive Inspection Integration.

For each program, we reviewed acquisition documents and interviewed program officials. To supplement our analysis, in addition to our sample, we also reviewed information from other DHS major acquisition programs obtained through prior and ongoing GAO reviews, such as the Financial Systems Modernization program. The programs' efforts provided illustrative examples of how acquisition risk management is implemented at DHS. To inform our work, we also reviewed acquisition risk management policies and guidance from DHS components that manage major acquisition programs to identify the variations across components. As of October 2022, eight components managed major acquisition programs: CBP, Coast Guard, Countering Weapons of Mass Destruction Office, Cybersecurity and Infrastructure Security Agency, FEMA, Management Directorate, Science and Technology Directorate, and TSA. We also interviewed relevant DHS and component officials.

To address our first objective, we compared DHS's acquisition risk management guidance to leading principles for acquisition risk management and federal internal control standards. We identified six leading principles for acquisition risk management based on a review of prior GAO work; the Project Management Institute, Inc.'s project management guide; and the Project Management Institute, Inc.'s standard for portfolio management.[4] We evaluated whether DHS's guidance broadly included the six leading principles for acquisition risk management at the program and portfolio levels. We also compared DHS's guidance and programs' efforts to federal internal controls on implementing control activities. Specifically, we evaluated whether DHS has documented through its policies how the agency will objectively assess risks and manage realized risks, which are risks that have

[4]GAO, *Enterprise Risk Management: Selected Agencies' Experiences Illustrate Good Practices in Managing Risk,* GAO-17-63 (Washington, D.C.: Dec. 1, 2016). Project Management Institute, Inc., *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)*, Sixth Edition (2017); and Project Management Institute, Inc., *The Standard for Portfolio Management*, Fourth Edition (2017). *PMBOK* is a trademark of Project Management Institute, Inc.

occurred.[5] We also described any supplemental acquisition risk management guidance that the components issued.

To address our second objective, we reviewed how DHS and the components shared risk management information across components and programs through data and document repositories and working groups. We compared these efforts to leading practices—which are recommended actions to implement leading principles—for lessons learned identified in prior GAO work.[6]

To address our third objective, we compared DHS's efforts to one leading principle for acquisition risk management—communication—and corresponding leading practices related to documentation and federal internal control standards.[7] We compared DHS's guidance and programs' efforts to federal internal controls in designing control activities—specifically, accurate and timely records—for certain types of program communications with stakeholders and leadership on acquisition risks.

Appendix I provides additional information on our scope and methodology.

We conducted this performance audit from September 2022 to August 2023 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.

[5]A risk has a percent likelihood of occurring, while a realized risk is a risk with 100 percent likelihood. DHS's acquisition risk management guidance refers to realized risks as issues.

[6]GAO, *Grants Management: OMB Should Collect and Share Lessons Learned from Use of COVID-19-Related Grant Flexibilities*, GAO-21-318 (Washington, D.C.: Mar. 31, 2021); *DOD Utilities Privatization: Improved Data Collection and Lessons Learned Archive Could Help Reduce Time to Award Contracts*, GAO-20-104 (Washington, D.C.: Apr. 2, 2020); *Project Management: DOE and NNSA Should Improve Their Lessons-Learned Process for Capital Asset Projects*, GAO-19-25 (Washington, D.C.: Dec. 21, 2018); and *Federal Real Property Security: Interagency Security Committee Should Implement a Lessons-Learned Process*, GAO-12-901 (Washington, D.C.: Sept. 10, 2012).

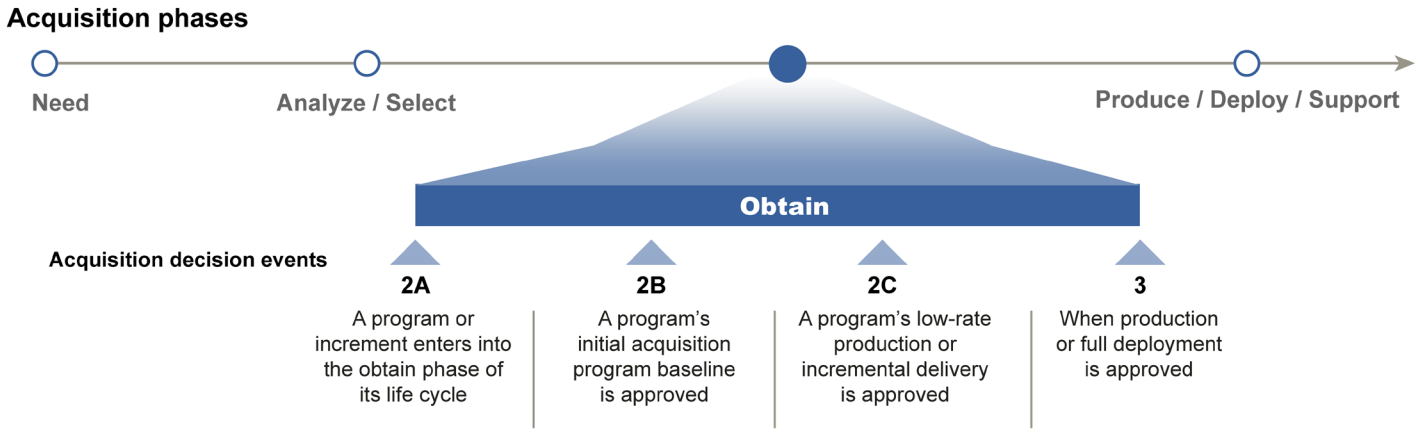
[7]The leading practice of communication was the most relevant to involving stakeholders and leadership.

Background

DHS Acquisition Risk Management

DHS's framework and process for managing its major acquisition programs are primarily set forth in its acquisition management directive and instruction (hereafter referred to as DHS acquisition policy).[8] DHS acquisition policy requires programs to manage their acquisition risks throughout the program's life cycle. As a program moves through its life cycle, it advances through a series of critical milestones called acquisition decision events, where DHS leadership assesses whether the program is ready to proceed to the next step (see fig. 1).

Figure 1: DHS Acquisition Decision Events in the Obtain Phase for Major Acquisition Programs



Source: GAO analysis of Department of Homeland Security (DHS) information. | GAO-23-106249

Several entities are responsible for supporting DHS's acquisition management function and have a role in how major acquisition programs conduct risk management:

- The **DHS Under Secretary for Management** serves as the acquisition decision authority for major acquisition programs and is responsible for reviewing each program at acquisition decision events. At each decision event, the decision authority assesses whether the program is ready to proceed to the next phase of its acquisition life

[8]DHS Directive 102-01, *Acquisition Management Directive* (July 28, 2015) (incorporating change 1, Feb. 25, 2019); DHS Instruction 102-01-001, Revision 02, *Acquisition Management* (Jan. 10, 2023).

cycle by reviewing and approving key acquisition documents. These key acquisition documents, including life-cycle cost estimates, testing plans, and program assessments, provide information on the program's acquisition risks.

- The **Acquisition Review Board** supports the decision authority in reviewing major acquisition programs at acquisition decision events and other meetings as needed. For the department's largest acquisition programs, the Under Secretary for Management chairs the board, which includes senior-level DHS members who represent various lines of business and expertise.[9] For example, the board includes the DHS Chief Financial Officer, Chief Procurement Officer, and Under Secretary for Science and Technology. Each board member and their staff use their subject matter expertise to provide input on a program's risks.
- **DHS PARM** is responsible for DHS's overall acquisition governance process, supports the Acquisition Review Board, and reports directly to the Under Secretary for Management. PARM develops and updates acquisition management policies and guidance, reviews major programs, and provides support to programs.
- The eight **components** oversee specific major acquisition programs.
  - **Component Acquisition Executives** are typically the most senior acquisition management official within each component and are responsible for overseeing the execution of their respective portfolios. The Component Acquisition Executives provide input on risks and monitor how programs manage these risks.
  - **Program offices**, also within the components, are responsible for planning and executing individual programs, which includes managing acquisition risks. Each program office is led by a program manager, who can appoint a **risk manager** responsible for facilitating risk management within the program. Risk manager responsibilities can include updating the program's risk management plan, leading risk management meetings, and tracking risks in a risk register—a central repository of risks.

[9]The Under Secretary for Management chairs the Acquisition Review Board for major acquisition programs with life-cycle costs of $1 billion or more as well as some programs with cost estimates between $300 million and $1 billion. The Under Secretary for Management can delegate their acquisition decision authority to Component Acquisition Executives for programs with cost estimates between $300 million and $1 billion.

In fiscal year 2019, DHS PARM took several actions to respond to our prior recommendations related to improving how DHS manages acquisition risks.[10] DHS PARM's actions—which apply to all major acquisition programs—included:

- Developing risk management guidance, including an October 2018 acquisition risk management guide, training, and templates for how programs track risks and present them to the Acquisition Review Board at acquisition decision events;[11]
- Revising DHS acquisition policy to require programs to submit a risk register, in addition to a previously required risk management plan, for component leadership review prior to acquisition decision events;[12]
- Hiring two risk management experts who work with components and programs to implement acquisition risk management; and
- Establishing a process for PARM's risk management experts to review and provide feedback to programs on their risk management plans, risk registers, and briefing materials to DHS leadership prior to acquisition decision events and program reviews.

After PARM's risk management policies, guidance, and processes went into effect, we still found gaps in how DHS programs implemented risk management. For example, in October 2020, we found that the Coast Guard's highest dollar acquisition program—the Offshore Patrol Cutter—did not track several key risks or how it was planning to mitigate its risks.[13] In June 2021, we found that the Management Directorate's Homeland Advanced Recognition Technology program did not identify the triggers that would indicate when a risk might be realized and require mitigation steps.[14] In these two reports, we recommended, among other actions, that the programs improve the information they used to manage risks, including comprehensively tracking risk management information

[10]GAO, *DHS Financial Management: Better Use of Best Practices Could Help Manage System Modernization Project Risks,* GAO-17-799 (Washington, D.C.: Sept. 26, 2017).

[11]DHS Office of Program Accountability and Risk Management, *Risk Management Training Aide for Acquisition Programs* (Oct. 9, 2018).

[12]DHS Instruction 102-01-001, Revision 02, *Acquisition Management* (Jan. 10, 2023).

[13]GAO-21-9.

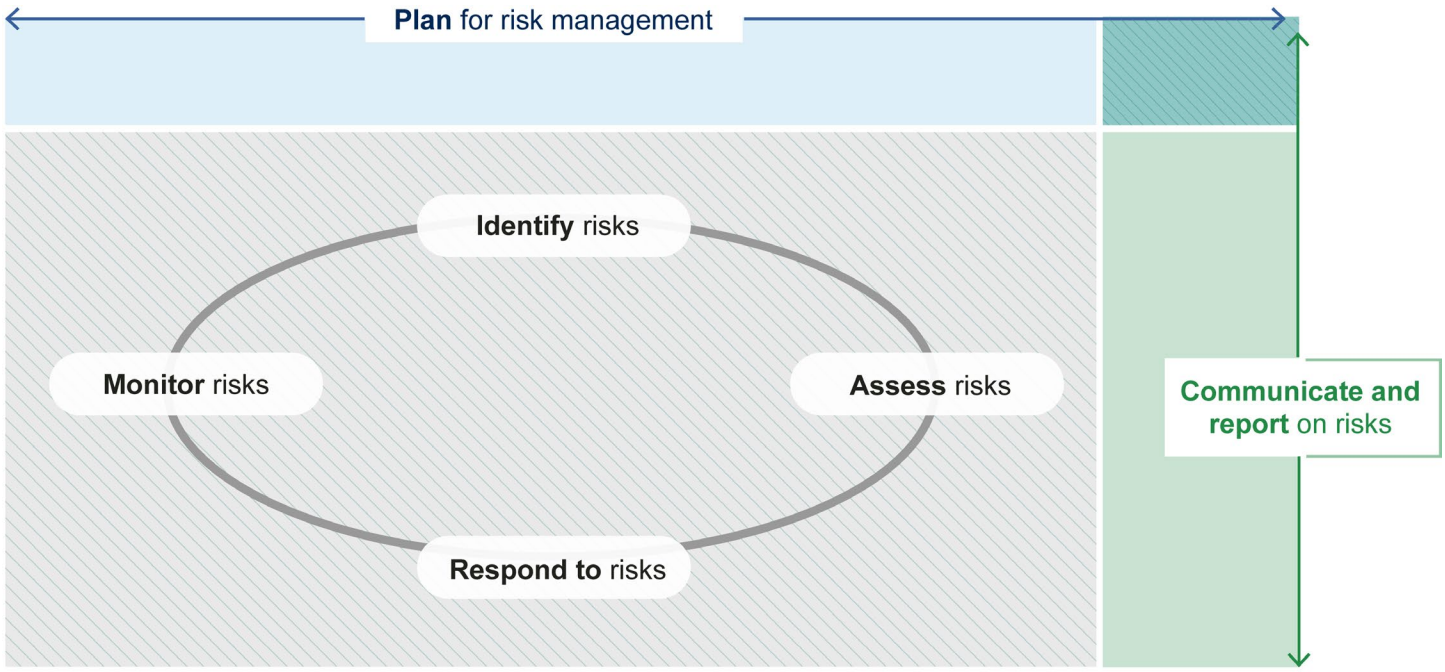
[14]GAO, *Homeland Security: DHS Needs to Fully Implement Key Practices in Acquiring Biometric Identity Management System,* GAO-21-386 (Washington, D.C.: June 8, 2021).

and maintaining accurate and current risk mitigation plans. DHS agreed with our recommendations and took steps to implement them.

Leading Principles in Acquisition Risk Management

We identified six leading principles of acquisition risk management, which should occur systematically and iteratively at both the program level and portfolio level (see fig. 2).[15]

Figure 2: Leading Principles for Acquisition Risk Management



Source: GAO analysis of GAO and Project Management Institute, Inc. information. | GAO-23-106249

Each of the six principles of acquisition risk management is described in more detail below:

- **Plan for risk management**. Programs should define their risk management process, including roles and responsibilities. A

[15]We identified six leading principles based on a review of GAO, *Enterprise Risk Management: Selected Agencies' Experiences Illustrate Good Practices in Managing Risk,* GAO-17-63 (Washington, D.C.: Dec. 1, 2016); Project Management Institute, Inc., *A Guide to the Project Management Body of Knowledge (PMBOK® Guide),* Sixth Edition (2017); and Project Management Institute, Inc., *The Standard for Portfolio Management,* Fourth Edition (2017). For more information on this analysis, see appendix I.

program's risk management plan should cover how the program intends to implement the five other principles.

- **Identify risks**. Programs should identify their risks and the risks' key characteristics.
- **Assess risks**. Programs should assess the likelihood and the impact of risks on their goals to help prioritize risk responses. Programs can perform subjective or objective risk assessments.
- **Respond to risks**. Programs should develop options for responding to the risks and select a risk response based on the assessments and prioritization of the risks and available resources.
- **Monitor risks and related responses.** Programs should monitor the implementation of the agreed-upon risk response action and evaluate how effective the response was for the risk.
- **Communicate and report on risks**. Programs should communicate throughout the risk management process with stakeholders and leadership. Communication on risks should occur throughout the other five principles.
    - **Engaging with stakeholders**. For the purposes of this report, the term stakeholders refers to subject matter experts who are independent from the program and provide inputs on risks and responses.[16] For example, DHS-level stakeholders include PARM, the Office of the Chief Financial Officer (including the Cost Analysis Division), the Office of the Chief Procurement Officer, and the Science and Technology Directorate's Test and Evaluation Division. Stakeholders can be external to the program, component, or DHS. We previously found that stakeholders who are independent can help to provide credible, objective, and unbiased conclusions.[17]
    - **Communicating with leadership**. For the purposes of this report, the term leadership refers to agency leadership that have acquisition oversight responsibilities. This includes the Acquisition

[16]DHS acquisition policy defines stakeholders as sponsors, users, and requirements managers. While engaging with users plays a critical role in ensuring the success of programs, we did not include user engagement in our analysis of stakeholder engagement.

[17]GAO-20-48G; and GAO, *Homeland Security Acquisitions: Opportunities Exist to Further Improve DHS's Oversight of Test and Evaluation Activities,* GAO-20-20 (Washington, D.C.: Oct. 24, 2019).

Review Board, the DHS Under Secretary for Management, and Component Acquisition Executives.

Each of the six leading principles for acquisition risk management encompasses a collection of leading practices that help programs implement the principle. For example, the Project Management Institute notes that when assessing risks, programs should acknowledge and correct for biases when they use subjective determinations. The Project Management Institute also highlights leading practices related to documenting risk inputs and outputs throughout the risk management process. This includes developing a risk management plan; recording risks, risk assessments, and responses in risk registers; and identifying relevant stakeholders in a stakeholder register.

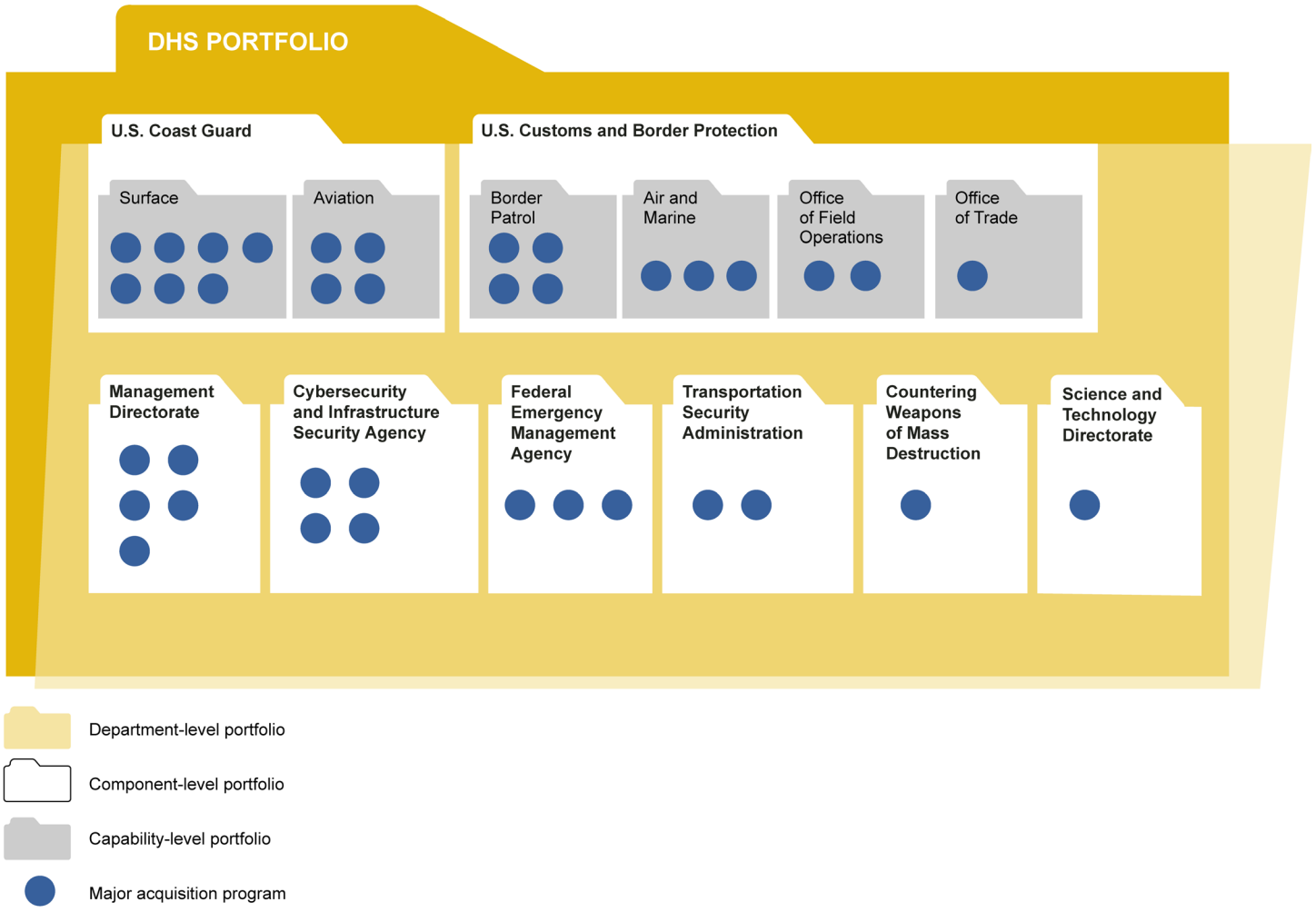
The six acquisition risk management principles apply to individual, program-specific risks, as well as collective, or portfolio-wide, risks. Portfolio management is a disciplined and integrated approach in which organizations view each of their investments as contributing to a collective whole, rather than independent and unrelated.[18] In 2018, we assessed DHS's policies for acquisition management, resource allocation, and requirements. We found that, when considered collectively, they generally reflected key portfolio management leading practices.[19]

Acquisition portfolios within DHS exist at multiple levels, including at the DHS-level, at the component-level, within components, and across components (see fig. 3).

[18]GAO, *Best Practices: An Integrated Portfolio Management Approach to Weapon System Investments Could Improve DOD's Acquisition Outcomes,* GAO-07-388 (Washington, D.C.: Mar. 30, 2007).

[19]GAO, *Homeland Security Acquisitions: Leveraging Programs' Results Could Further DHS's Progress to Improve Portfolio Management,* GAO-18-339SP (Washington, D.C.: May 17, 2018).

Figure 3: Notional Depiction of How DHS's Acquisition Portfolios Exist at Multiple Levels



Source: GAO analysis of Department of Homeland Security (DHS) information. | GAO-23-106249

Note: The figure does not comprehensively include all of DHS's acquisition portfolios, including capability-level portfolios that span across components. The number of major acquisition programs is as of October 15, 2022. In addition to major acquisition programs—programs with life-cycle costs of $300 million or more—DHS and the components also manage non-major acquisition programs—programs with life-cycle costs less than $300 million—within their portfolios. Non-major acquisition programs are not reflected in the figure.

As a result, staff responsible for managing portfolios, or portfolio managers, may oversee multiple programs across components at the DHS-level, within a component, or within a specific capability-level portfolio. Risk management at the portfolio-level requires portfolio

managers to consider risks beyond individual programs. For example, portfolio risk management considers:

- **Enterprise-level risks** that affect multiple programs across the portfolio, such as COVID-19 effects on the supply chain or cybersecurity vulnerabilities.
- **Interdependency risks**, in which risks from one program affect another program's risks and preferred risk responses. For example, programs that interface with each other to jointly deliver a capability may face schedule risks if one of the programs is delayed.

DHS Addresses Leading Principles of Acquisition Risk Management but Lacks Guidance on Some Key Practices

DHS's acquisition risk management guidance broadly includes the six leading principles of acquisition risk management for programs. However, DHS's guidance does not include specific methods for programs to implement some of DHS's own risk management goals. DHS's guidance and selected programs also fall short on addressing leading principles for acquisition risk management at the portfolio-level. DHS plans to update its acquisition risk management guidance by fall 2023, which presents an opportunity to address the gaps we identified.

DHS Guidance Includes Leading Principles of Acquisition Risk Management at the Program Level

DHS PARM's October 2018 risk management guide and related guidance include detailed instructions for acquisition programs on how to implement the six leading principles for acquisition risk management that we and the Project Management Institute have identified (see table 1).

Table 1: Leading Acquisition Risk Management Principles and Corresponding Instructions in DHS Guidance

Leading principle	Examples of how DHS guidance includes principle
Plan for risk management	Asks programs to develop a risk management plan that addresses how the program will implement each of the other risk management principles, including identifying roles and responsibilities of the risk manager, risk tracking tools used, and how often the risk management teams will meet
Identify risks	Asks programs to document risks in a risk register—a centralized repository of risks—including the assigned risk owner, description, and trigger (indicator that a risk will be realized); and to document how the program is implementing other leading principles, such as risk responses
Assess risks	Asks programs to develop risk statements that include a description of why the program is tracking the risk, the likelihood of the risk occurring, the impact to the program's cost, schedule, and performance objectives if the risk is realized, and rationale for the risk likelihood and impacts selected
Respond to risks	Asks programs to select a response from four options: avoid, transfer, mitigate, and accept; and to develop plans to manage risks

Leading principle	Examples of how DHS guidance includes principle
Monitor risks and related responses	Asks programs to update risk register regularly; document planned and actual dates for completing risk responses for all high and medium risks; and track risk triggers
Communicate and report on risks	Asks programs to present all high and selected medium risks (at the program's discretion) at Acquisition Review Board meetings

Source: GAO analysis of GAO; Project Management Institute, Inc.; and Department of Homeland Security (DHS) information. | GAO-23-106249

Component officials described DHS PARM's risk management guidance as clearly written and easy to understand. Component and program officials also expressed that they found the guidance to be valuable and appreciated that it was not overly prescriptive. DHS PARM officials stated that the guidance provides helpful direction, while still providing programs with flexibility to tailor their risk management approaches.

Further, five of the eight components—CBP, Coast Guard, Countering Weapons of Mass Destruction Office, Cybersecurity and Infrastructure Security Agency, and TSA—issued acquisition risk management guidance to supplement DHS PARM's guidance. Components' guidance covers topics such as managing stakeholders, managing realized risks, and risk tolerance. For example, CBP's supplemental guidance emphasizes risk tolerance and describes management approaches that reward innovation. CBP's guidance also describes the role of CBP's Chief Risk Officer, who is responsible for establishing risk tolerance procedures. Another component, the Cybersecurity and Infrastructure Security Agency, has supplemental guidance that includes templates for managing stakeholder engagement. These templates encourage programs to track relevant stakeholders in a register, assess stakeholder involvement, and establish preferred communication channels.

Three of the eight selected components—FEMA, the Management Directorate, and the Science and Technology Directorate—have not issued supplemental acquisition risk management guidance. Officials from these components explained that their programs use DHS PARM's guidance, which is sufficient for their purposes. Appendix II provides descriptions of each component's supplemental risk management guidance.

DHS Guidance Lacks Specificity for Conducting Certain Risk Assessments and Managing Risks that Have Occurred

DHS guidance does not effectively address how programs can achieve some of DHS's own risk management goals—namely (1) assessing risks, one of the leading principles, in an objective manner, and (2) managing realized risks, which are risks that have occurred. Federal internal control standards state that agencies should implement control activities—such as documenting through policies how the agency will achieve its goals and address risks.[20] If an agency's policy does not provide enough information on how it will achieve a key goal, then the agency might need to improve existing or implement additional controls.

DHS Guidance Does Not Address Methods for Objectively Assessing Risks

DHS PARM's acquisition risk management guidance emphasizes that assessing risks—one of the six acquisition risk management leading principles—in an objective manner is important for informed decision-making. The guidance states that consistent pre-defined parameters provide a structured means for evaluating risks so decision makers and program office staff can make objective comparisons. As much as possible, officials should base the likelihood and consequence ratings on objective, quantitative criteria.[21] The resulting risk assessments—whether a risk is high, medium, or low—drive how the programs respond to and communicate the risks. For example, as noted earlier, DHS PARM's guidance states programs should report on all high risks to DHS leadership prior to acquisition decision events.

However, the guidance generally does not identify methods for how programs can achieve DHS's goal of objectively assessing risks. Our analysis of programs' efforts, risk management leading practices, and prior GAO work identified several examples of methods programs could take to conduct objective risk assessments:

- **Applying business rules**. Business rules can help a program objectively identify when it needs to add a risk to the risk register. For example, the risk management plan for the selected TSA program outlines business rules that objectively identify and prioritize schedule and cost risks. The risk management plan notes that a program's integrated master schedule weekly report prompts the identification of risks when a business rule—for example, if a contract award moves into the last quarter of the fiscal year—is triggered. At that point, the integrated master schedule team flags the activity and provides the

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

[21]DHS Office of Program Accountability and Risk Management, *Risk Management Training Aide for Acquisition Programs* (Oct. 9, 2018).

information to the program manager for input into the program's risk register.

- **Acknowledging biases in subjective risk assessments**. Leading practices from the Project Management Institute include acknowledging and correcting for biases when subjective determinations of risks are used. This includes documenting explanatory details for how officials assigned risk levels, including the assumptions underpinning a risk assessment.
- **Using stakeholders to help assess risks**. Stakeholders who are independent from the program can help objectively assess risks. We previously found that having an "honest broker" who is independent of the program can mitigate against a program office's optimism—optimism that can lead to underestimating risks.[22] Similarly, we previously found that objectivity is a key characteristic to high-quality technology readiness assessments, which help to uncover technology risks.[23] This objectivity is achieved by including staff who are free from internal and external bias or influence—typically, staff who are outside of the program office.

DHS officials acknowledged that programs often arrive at the risk levels subjectively, explaining that objective assessments of risks are challenging to conduct and resource-intensive. As a result, subjective determinations are common and expected. Similarly, officials from a Financial Systems Modernization program stated that estimating the probability and impact of risks in a consistent, objective manner is difficult, which leads to subjective determinations.

We found examples of programs that missed opportunities to improve the objectivity of their risk assessments, which as mentioned, is emphasized in DHS guidance:

- The risk management plans for four programs we reviewed did not include business rules to operationalize any risk triggers included in the plans. Further, one of these risk management plans did not include quantitative metrics to help distinguish whether risks should be designated as high, medium, or low. Specifically, officials from our selected Cybersecurity and Infrastructure Security Agency program explained that instead of using quantitative metrics, they instead rely on the collective expertise of the risk team to assign risk levels.

[22]GAO-20-195G.

[23]GAO-20-48G.

- Two programs we reviewed did not document how they arrived at the risk levels they assigned to specific risks, which obscures how any assumptions or biases may have affected the subjective risk assessments.
- Officials from two DHS-level stakeholder offices that we interviewed—Cost Analysis Division and Office of the Chief Procurement Officer—stated that while they have the capacity to assist programs in assessing risks, programs generally have not requested such assistance.

While objective risk assessment may not be possible or warranted for all risks, programs can underestimate their risks if they do not have additional guidance on how they can improve the objectivity of their risk assessments. Not objectively evaluating risks, in turn, may hinder a program's ability to appropriately prioritize and respond to risks and obscures DHS leadership's insight into the most significant risks.

DHS Provides Minimal Guidance on Approaches for Managing Realized Risks

DHS PARM's acquisition risk management guidance emphasizes the importance of distinguishing between risks and realized risks.[24] The guidance indicates that realized risks should be managed differently and includes some information related to methods for managing realized risks:

- **Planning for realized risks**. DHS PARM's guidance states that programs should develop plans to reduce the impact of risks once they occur.
- **Identifying realized risks**. DHS PARM's guidance states that programs should document realized risks in risk registers. DHS PARM's risk register template asks programs to include expected impacts, status dates and updates, and plans to manage each realized risk.
- **Communicating realized risks**. DHS PARM's guidance states that programs should report realized risks to the Acquisition Review Board at acquisition decision events. DHS PARM's template for briefing the Acquisition Review Board asks programs to report on what caused the risk to occur and any mitigation activities.

However, DHS PARM's guidance does not address the specific steps programs should take to monitor and respond to risks once they have been realized. We found several instances in which programs missed opportunities to better manage and communicate about realized risks:

[24]DHS's acquisition risk management guidance refers to realized risks as issues.

- **Not identifying realized risks and their impacts in risk register**. Our analysis found that the selected Coast Guard program did not add realized risks related to deficiencies with its contractor's business systems to its register. Program officials explained that they only track realized risks that they had previously identified as risks, which did not include contractor business system deficiencies. Officials further explained that while they did not track these realized risks in the risk register, they were working with the contractor to address the business system challenges outside of the risk management process. The program also did not track any additional risks resulting from the realized risks, such as unreliable contractor data that affect the program's ability to manage and oversee the contract.

  Further, the selected Cybersecurity and Infrastructure Security Agency program did not identify any realized risks in the register reviewed by DHS PARM leading up to a decision event. After DHS PARM noted the absence of realized risks, program officials added a realized schedule risk that resulted from funding challenges to their register prior to the Acquisition Review Board meeting.

- **Not fully documenting management of realized risks**. We also found that DHS PARM identified limitations in how the TSA program we selected documented active management of several realized risks in its risk register. For example, DHS PARM found that several realized risks lacked the details necessary for managing their impact to the program. Similarly, for the selected CBP program, PARM officials identified that the program needed to update its plan to manage an affordability risk once it was realized. Both programs updated their risk information in response to DHS PARM's feedback.

DHS PARM officials stated that they plan to update their risk management guidance by fall 2023 to include additional information on the differences between managing risks and managing realized risks. However, officials were still determining what they plan to include in the guidance. Officials have not yet determined whether the update would include how realized risks generate additional risks or additional guidance for how programs should assess and respond to realized risks. As DHS works to update its guidance, including additional direction on realized risks can ensure programs are better positioned to respond to risks once they have occurred, which may help to improve program outcomes.

DHS's Guidance and Approaches Do Not Address Leading Principles for Portfolio Risk Management

Leading principles we previously identified recommend that agencies manage the combined effect of risks as an interrelated portfolio rather than addressing risks only within silos.[25] The Project Management Institute notes that facilitating the prioritization of portfolio resources may not always align with the goals of risk management at the program level. The Project Management Institute also identifies specific practices for implementing portfolio risk management.

However, DHS PARM's risk management guidance does not address how portfolio managers should implement risk management at the portfolio level, as found in leading principles. Our analysis found examples of certain leading practices within the planning, identifying, and communication leading principles that DHS PARM's guidance does not address:

- **Planning for portfolio risk management**. The Project Management Institute emphasizes the importance of delegating portfolio-level responsibilities and identifying portfolio risk owners. The Project Management Institute also recommends the use of a portfolio-level risk management plan. However, DHS PARM's guidance does not address designating and documenting responsibilities for portfolio risk management, for example, in a program's risk management plan. In contrast, the selected CBP program's risk management plan outlines the responsibilities for the portfolio risk manager, which include identifying recommendations to address enterprise-level risks that affect multiple programs and raising interdependency risks.
- **Identifying portfolio-level risks in risk documents**. The Project Management Institute acknowledges that risks across different parts of the same organization can interact, and that portfolio managers should be aware of such interdependencies to manage risks. For example, a program may choose to accept a schedule risk because it deems the cost to mitigate the risk to be too high. However, the portfolio manager may recognize that another program will have to incur even higher costs to further sustain a needed capability given the delay. In this example, while it is costly for the first program to mitigate the schedule risk, it may be worth the cost at the portfolio-level. However, DHS PARM's guidance does not address identifying and documenting portfolio-level risks. For example, it does not direct portfolio managers to highlight portfolio risks in risk documentation, such as a portfolio-level risk management plan. In contrast, the FEMA

[25]GAO-17-63.

program we selected identifies risks with interdependencies that affect other programs in its risk register.

- **Communicating how risks may affect other programs.** The Project Management Institute emphasizes the importance of including leadership and other stakeholders in portfolio risk planning and identification. While DHS PARM's guidance acknowledges portfolio-level considerations in communicating interdependency risks to leadership and other stakeholders, it does not ask programs to present on portfolio risks during Acquisition Review Board meetings. The guidance also does not identify mechanisms for portfolio managers to (1) consistently communicate interdependency risks, and (2) inform other affected programs of these risks at pre-determined intervals or at particular cost or schedule thresholds.

We found examples across our selected programs of the importance of having responsibilities and processes in place for accounting for portfolio-level risks:

- According to officials, the selected CBP program had a portfolio risk manager who moved to a different position. Following our inquiries, program officials told us that they realized the ratings for certain risks were not current and accurate because they did not reflect broader program considerations that had arisen after the portfolio risk manager left and while the position remained vacant. These officials told us they are in the process of reassessing the risks and acknowledged that a portfolio risk manager is helpful in ensuring risk assessments are informed and account for portfolio-level considerations.
- The schedule risks for the selected Coast Guard program increased the cost risks for the *Polar Star* service life extension program, a non-major Coast Guard acquisition program. Program officials stated that interdependency of the acquisition risks between these two programs are communicated to leadership during regular meetings as needed, on an ad hoc basis. However, the selected Coast Guard program did not identify or assess the interdependency risks in its risk register to inform stakeholders. Additionally, despite the aggressive schedule of the selected program, the portfolio manager of these programs did not conduct portfolio-level risk assessments.
- Officials from the selected TSA program described an interdependency risk related to software updates from another TSA program. Program officials stated that they eventually developed a strategy to mitigate this risk. However, they did not do so until they proactively reached out to the other program.

In another case, DHS officials acknowledged that there are interdependency considerations between CBP's Biometric Entry-Exit program and Management Directorate's Homeland Advanced Recognition Technology program. According to Management Directorate officials, their program provides leadership with quarterly status briefings, and CBP representatives participate in these briefings. However, during the course of our review, officials from the CBP program reported that they are currently unaware of what risks and realized risks are being tracked by the Management Directorate's program.

DHS PARM officials explained that they have not issued portfolio risk management guidance because they want components and programs to have flexibility in managing portfolio-level risks, and they expect components to have their own guidance. However, the component-level supplemental risk management guidance noted earlier provides varying levels of information on portfolio risk management.[26] For example:

- Supplemental guidance from three of the five components emphasizes that programs should be aware of enterprise-level risks, and in some cases assigns responsibilities for reviewing such risks.
- Two of the five components with supplemental risk management guidance identified positions that are responsible for aspects of portfolio risk management, but their guidance does not specify how those positions should manage risks across portfolios.
- None of the component-level supplemental risk management guidance describes processes for identifying and communicating risks associated with other components' programs.

Component and program officials also stated that they typically identify portfolio-level risks and communicate on an ad hoc basis. For example, FEMA officials explained that programs are able to share information about interdependency risks during regular program manager meetings. However, officials from two components agreed that having additional guidance for portfolio risk management would be helpful to ensure consideration of portfolio risks. Additionally, the components' supplemental guidance does not address DHS-wide considerations for identifying and communicating portfolio-level risks across components.

[26]As noted earlier, five components have supplemental acquisition risk management guidance, and the three other components do not.

Without additional guidance on portfolio risk management, portfolio managers may not have timely or full visibility into portfolio-level risks, which hampers their ability to effectively manage these risks or make fully informed decisions that optimize the portfolio's resources.

DHS Has Not Weighed Costs and Benefits of Implementing a Tool to Facilitate Risk Knowledge-Sharing

DHS has not assessed the costs and benefits of implementing a DHS-wide tool to store and share knowledge that programs could use to facilitate how they implement risk management at both the program and portfolio levels. In prior work, we found that the collecting and sharing of lessons learned from previous programs provides organizations with a powerful method for sharing ideas for improving work processes.[27] A central component of a successful lessons learned process is to ensure that lessons learned are stored in a logical, organized manner.

We also found that relying on person-to-person discussions to share lessons learned can be problematic because personal networks can dissolve—for example, through attrition—and informal information sharing does not ensure everyone is benefiting from the lessons that are gleaned.[28] Additionally, as noted earlier, leading practices recommend that agencies manage the combined impact of risks as an interrelated portfolio rather than addressing risks only within silos. Such portfolio risk management is achieved through information-sharing among programs.

Our analysis of programs' risk management approaches identified examples of helpful risk knowledge and lessons learned that generally remained siloed within a program or sporadically shared in ad hoc forums:

Data on program risks and related risk responses. As programs track their risks and subsequent responses in risk registers, they generate valuable data for risk management. For example, the five programs we reviewed all tracked data on how effective various risk responses were at addressing risks and the length of time needed to address certain risks.

Program officials identified examples of how they effectively leveraged risk data to inform their risk management activities. Officials from our selected TSA program explained that they track program actions that are historically effective at mitigating a particular risk so that they can use the same ideas to mitigate future risks. For example, TSA program officials

[27]GAO-21-318; GAO-20-104; GAO-19-25; and GAO-12-901.

[28]GAO-19-25; and GAO-12-901.

stated that based on prior risk mitigation efforts, they now release smaller batches of units at initial deployment to minimize the risk of rework if problems are discovered later. Similarly, officials from our selected CBP program told us that they reviewed risk responses from another CBP program's risk register to inform how they responded to similar risks.

Risk management approaches and lessons learned. Programs we reviewed also provided examples of how they tailored their risk management approaches, which they shared as lessons learned to inform other programs' risk management approaches. For example:

- As a program using Agile development principles, the selected FEMA program uses an Agile framework—which emphasizes iterative product development and delivery that are continuously evaluated on quality and other objectives—to manage its acquisition process.[29] The program applies this same framework to its risk management approach. FEMA component officials stated that they encouraged the selected FEMA program to collaborate with another FEMA program using Agile to share lessons learned from its Agile risk management approach. For example, the program holds biweekly 30-minute risk meetings to cover the most urgent risks rather than comprehensively cover all risks. The program also enters risks into the register before it has complete information to help the program quickly see new risks.
- The selected Cybersecurity and Infrastructure Security Agency program is highly interdependent with two other programs in the emergency communications division. The three programs conduct some risk management activities jointly. For example, the programs hold monthly risk meetings that include all three programs given how interrelated the programs' risks are.

DHS does not have a department-wide repository to store and share knowledge that programs and portfolio managers could use to implement acquisition risk management, including leading practices in portfolio risk management. Instead, DHS, the components, and programs have shared risk information on an ad hoc basis during meetings. For example, since November 2021, DHS PARM has held two risk management working groups that included participants from all eight components that manage major acquisition programs. During these meetings, DHS PARM officials shared leading practices, provided an overview of DHS PARM's role in

[29]For more information on Agile software development, see GAO, *Agile Assessment Guide: Best Practices for Agile Adoption and Implementation,* GAO-20-590G (Washington, D.C.: Sept. 28, 2020).

assisting programs with risk management, and invited program officials to present on the benefits and drawbacks of various risk tracking tools. DHS PARM officials stated that they plan to hold the working groups every 6 months in the future but the frequency may be less given the topical nature of the meetings. Additionally, participation in the working group is voluntary. As a result, while the working groups are a positive step, they are not sufficient for ensuring risk knowledge is systematically stored and shared for future use.

Further, programs across DHS currently use a variety of risk tracking tools or manually-completed spreadsheets, which do not facilitate information sharing across the department (see table 2).

Table 2: Examples of Risk Tracking Tools by DHS Component

Component	Number of major acquisition programs, as of October 2022	Tools used by programs to track risks cited by component officials			
		Active Risk Manager[a]	Microsoft Excel[b]	Microsoft SharePoint[c]	Jira[d]
U.S. Coast Guard	11	—	X	—	—
U.S. Customs and Border Protection	10	X	X	X	X
Management Directorate	5	X	X	X	—
Cybersecurity and Infrastructure Security Agency	4	—	X	—	X
Federal Emergency Management Agency	3	—	X	—	X
Transportation Security Administration	2	—	X	—	—
Countering Weapons of Mass Destruction Office	1	—	—	X	—
Science and Technology Directorate	1	—	X	—	—

Legend: X = Yes — = No

Source: GAO analysis of Department of Homeland Security (DHS) information. | GAO-23-106249

Note: The commercial tools cited in the table should not be construed as an affiliation with, endorsement of, or sponsorship by GAO of these commercial tools.

[a]Active Risk Manager is web-based, risk management software that automates certain risk reporting and portfolio-level analysis, and requires licenses for use.

[b]Microsoft Excel is software that allows users to enter and organize risks in spreadsheets that are generally static.

[c]Microsoft SharePoint is web-based software that allows users to store, organize, and access risk information across devices.

[d]Jira is cloud-based, risk management software that automates certain risk reporting and portfolio-level analysis, and requires fees for certain functions.

While commercially available risk tracking tools have the capability to share data across programs, officials explained that one of the benefits of using manually-completed spreadsheets is that there are no licensing costs, unlike other tools. However, officials acknowledged that information in such spreadsheets remains siloed. Further, while DHS PARM recently launched its Acquisition Data Analytics Platform Tool to help DHS's acquisition community manage and oversee programs, PARM officials do not currently plan to include risk data and documentation as part of the tool's rollout of future capabilities. Officials explained they were focused on the successful rollout of priority functions, such as facilitating immediate access to key acquisition documents and their data elements.

However, component and program officials told us that systematically sharing risk data and approaches, such as through a DHS-wide risk tool, could benefit programs in their day-to-day risk management and facilitate portfolio risk management. For example:

- Component officials from the Cybersecurity and Infrastructure Security Agency stated that they are contemplating developing a component-wide risk register that programs could go to for a one-stop shop of risk data. Officials stated that such a tool could potentially inform leadership of risks in a more efficient way, provide better analytics and trends, and thus provide better management oversight and insight across the component. Similarly, component officials from the Countering Weapons of Mass Destruction Office stated that they see a need to create a portfolio-level risk tool to have better insight into interdependency risks.
- Officials from the selected TSA program stated that while they feel comfortable reaching out to DHS PARM for risk management guidance, the centralization of knowledge and expertise from DHS PARM's risk management experts would be helpful in preserving institutional knowledge.
- Officials from the selected FEMA program stated that they have found their commercial risk tracking tool to be more helpful than static and siloed spreadsheets because it allows the program to store risk data that it can share with other programs.

DHS PARM officials stated that they have not required programs to use a department-wide risk tracking tool because this could hamper programs' ability to tailor their risk management frameworks to fit their needs and resources. However, DHS PARM has not assessed whether the benefits of such a tool, such as the ability to more effectively conduct portfolio risk management, outweigh the costs, including the potential for reduced

program flexibility and any monetary costs with obtaining licenses or acquiring such a tool.

The DHS Cost-Benefit Analysis Guidebook states that a cost benefit analysis is a proven management tool that assists in planning and managing costs and risks. Assessing the costs and benefits of a department-wide risk tracking tool would provide DHS with greater insights into whether the assumed costs outweigh the benefits.

Selected Programs Engage with Stakeholders and Leadership on Risk Management but Do Not Consistently Document This Involvement

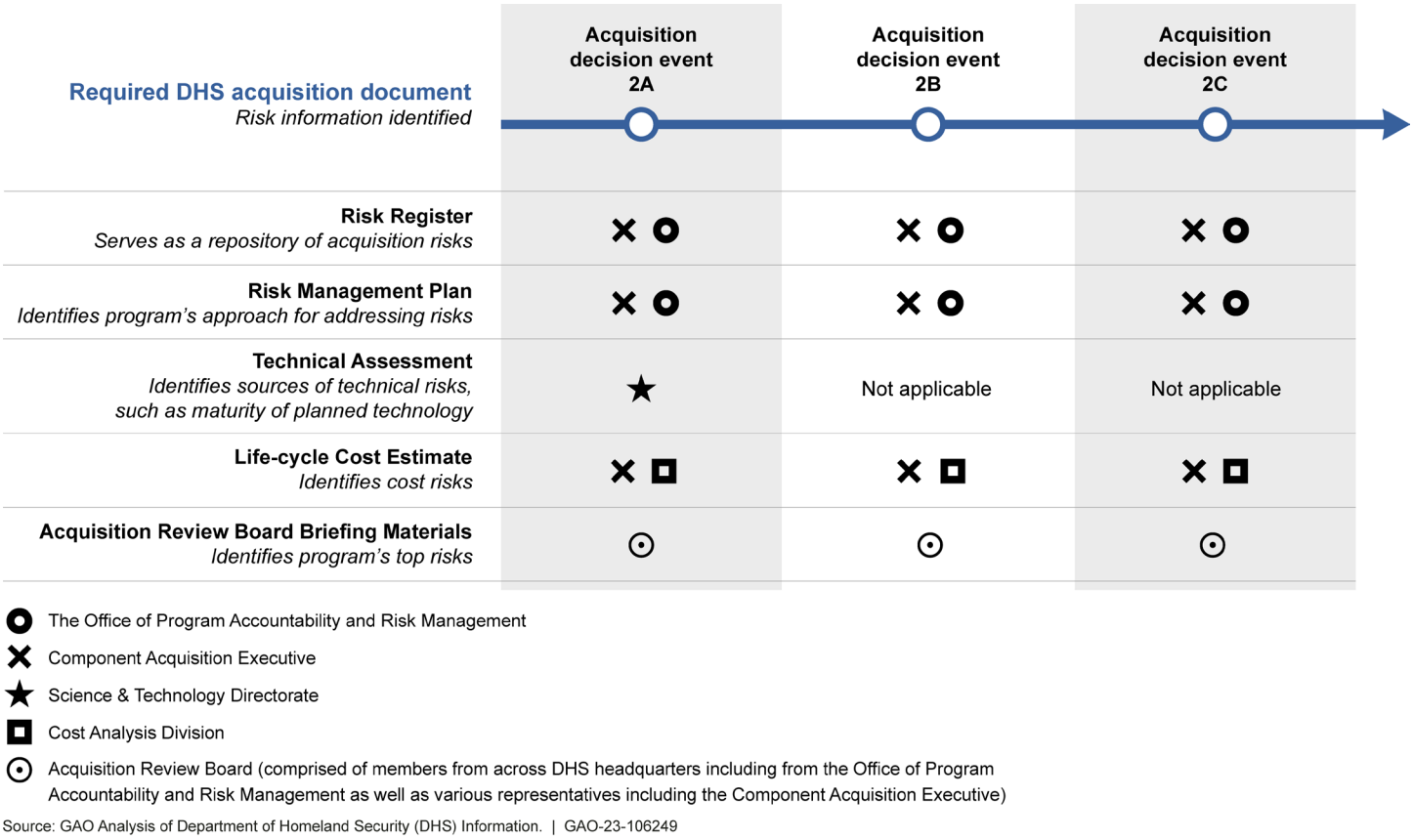
DHS acquisition risk management guidance encourages programs to engage with stakeholders and leadership throughout their acquisition life cycles. We found examples of this engagement as programs prepared for acquisition decision events. However, we also found gaps in DHS guidance and programs' approaches for ensuring that they incorporate stakeholder inputs on risks and communicate current risk information to leadership.

DHS Guidance and Programs' Approaches Include Stakeholder and Leadership Engagement on Risks

DHS acquisition policy and DHS PARM risk management guidance direct programs to engage with stakeholders and leadership on their risks throughout the acquisition process, especially prior to acquisition decision events. The DHS-level Acquisition Review Board, component-level leadership, and stakeholders have multiple opportunities to review and provide input on program risks—such as through the development and review of key acquisition documents—prior to acquisition decision events.

Key acquisition documents that involve stakeholder input include the life-cycle cost estimate, technical assessment, and other program assessments. For example, DHS's Cost Analysis Division can raise risks related to program costs in the life-cycle cost estimate. Additionally, meetings such as the pre-Acquisition Review Board briefing provide forums for leadership and stakeholders to raise concerns about program risks (see fig. 4).

Figure 4: Examples of Required Program Documents with Risk Information that DHS Leadership and Stakeholders Review throughout the Acquisition Life Cycle



Source: GAO Analysis of Department of Homeland Security (DHS) Information. | GAO-23-106249

In addition to these opportunities, leadership can gain knowledge about program risks from quarterly Acquisition Program Health Assessment reports and regular meetings with Component Acquisition Executives, which are outlined in DHS acquisition policy. Various stakeholders within DHS conduct quarterly Acquisition Program Health Assessment reports to assess categories such as schedule, technology, and contract management.

Further, the component-level supplemental risk management guidance noted earlier also addresses stakeholder engagement. For example:

- The Cybersecurity and Infrastructure Security Agency issued stakeholder guidance that assists programs in identifying and

engaging with stakeholders during risk management, as well as documenting such interactions.

- The Coast Guard's risk management guidance highlights the importance of stakeholder engagement. This includes coordinating with appropriate stakeholders during risk mitigation planning, obtaining stakeholder concurrence with risk mitigation actions, and providing a list of tracked risks to the affected stakeholders.

We found examples of programs demonstrating stakeholder engagement as part of their risk management approaches in three main ways:

Incorporating risks identified by stakeholders. Two programs identified examples of stakeholder subject matter expertise helping them to identify risks that they did not originally consider. For example:

- In January 2023, a TSA testing official voiced concerns about the selected TSA program's testing environment not functioning correctly in preparation for an operational test event. Program officials stated that once the testing office communicated this risk to them, they began tracking it in the risk register. As a result, the program developed plans to mitigate the risk until it discovered and implemented a solution to stabilize the testing environment.
- During a pre-Acquisition Review Board meeting in March 2022, a senior Navy official raised concerns about the selected Coast Guard program's plans for a new control system. After the official raised concerns, the program added this risk to its risk register in April 2022 and chose to mitigate the risk. The program plans to set up a testing facility to ensure that the control system is fully functional.

Addressing stakeholder-identified risks prior to acquisition decision events. DHS PARM officials identified an example of a program not included in our sample where stakeholders provided input that delayed the program's acquisition decision event until the program reduced risks to an appropriate level. As FEMA's Enterprise Data and Analytics Modernization Initiative program prepared for an acquisition decision event in 2021, two stakeholder offices shared concerns about the program in a required technical assessment. Specifically, DHS PARM officials stated that the Office of the Chief Information Officer and Office of Systems Engineering found that the program had not adequately planned the systems engineering methodology to support the decision event. The program delayed its decision event and established a systems engineering working group in coordination with these stakeholders to identify and document next steps. According to DHS PARM officials, the

program addressed the risk areas and achieved its acquisition decision event in June 2022.

Regular meetings with stakeholders. All five of the programs we reviewed shared that they engaged with stakeholders through working-level risk management activities. For example:

- **Including stakeholders in risk management meetings**. According to officials, the selected FEMA program holds biweekly meetings to review program risks. Program officials told us that they invite stakeholders to these meetings as needed to provide their subject matter expertise on risks.
- **Conducting ad hoc outreach to stakeholders**. Officials from several programs stated that when they have risk management questions, they contact DHS PARM's risk management experts directly. These officials described these experts as helpful and knowledgeable.

Officials from three DHS-level stakeholder offices we spoke with stated that programs involve their offices as needed and that they generally do not face challenges engaging with programs. For example, DHS's Cost Analysis Division stated that the selected CBP program engaged with their office prior to an acquisition decision event as part of the independent cost analysis process. Officials stated that this was the appropriate time for the cost division to conduct a review and provide input on the program's funding risk. Similarly, the Test and Evaluation Division shared that officials have collaborative discussions with programs based on results from testing that can uncover risks to operations.

The programs we reviewed also engaged with leadership on a regular basis, and highlighted the importance of leadership support as a key element of successful risk management. Several program officials stated that their respective leadership fosters a culture in which they can raise risks without fear. Component officials explained that leadership prefers to know about risks sooner rather than later because "surprises are bad in this line of business." CBP component officials shared that if their Component Acquisition Executive sees that a program has only low risks, that official would question whether the program was accurately representing its risks or whether the program had full visibility into its risks. Additionally, officials from the selected FEMA program stated that they do not want to "blindside" any stakeholders at an Acquisition Review

Board meeting with new risks that the program had not previously discussed with relevant stakeholders.

Selected Programs Did Not Consistently Ensure Stakeholder Input Was Tracked or Incorporated

DHS PARM risk management guidance and program approaches do not fully reflect leading practices related to incorporating and documenting stakeholder input—practices within the communication leading principle. The Project Management Institute suggests identifying stakeholders regularly, such as in a stakeholder register, and analyzing and documenting stakeholder engagement, such as in a stakeholder engagement plan.[30] The leading practices further state that organizations can better manage risks by sharing risk information and incorporating feedback from stakeholders. Further, as noted earlier, having an "honest broker" who is independent of the program can mitigate against a program office's optimism. This optimism can lead to an underestimation of risks.[31]

We identified a number of instances when programs' risk management approaches did not align with leading practices related to documenting stakeholders' input or for fully considering stakeholders' engagement. For example:

Identifying stakeholder input in the risk register. According to DHS PARM officials, the risk register is meant to be a traceable and historical document for the program to reference in the future. However, our analysis found two programs that did not consistently identify which stakeholders provided input in their risk registers.

For example, the selected CBP program included a realized risk in its risk register related to program funding. According to DHS PARM officials, as the program moved toward an acquisition decision event, DHS's Cost Analysis Division helped determine that the program needed to update its certification of funds memorandum to better encompass the strategy for addressing the program's realized funding risk. Despite this close coordination, we were unable to identify documentation of this stakeholder's input in the risk register.

[30]Project Management Institute, Inc., *A Guide to the Project Management Body of Knowledge (PMBOK® Guide),* Sixth Edition (2017); and Project Management Institute, Inc., *The Standard for Portfolio Management*, Fourth Edition (2017).

[31]GAO-20-195G.

Similarly, Management Directorate officials described challenges identifying whether stakeholders had provided input into one program's risk registers. Officials shared that for the Financial Systems Modernization program, stakeholders tend to manage risks in an informal manner without fully adding information into the risk register. They stated that this makes it harder for the program and component to track the progress in identifying root causes of a risk, mitigating a risk, and avoiding future risks.

Engaging stakeholders in the risk management process. We found that while the selected Coast Guard program engaged with various Department of Defense stakeholders to address its contractor business system challenges, the program did not directly engage with certain stakeholders throughout the risk management process. Specifically, the program included two contractor oversight offices in its risk management meetings. According to program officials, these oversight offices coordinated with Department of Defense contract auditing offices that identified deficiencies with two of the contractor's business systems. However, the program did not involve these contract auditing offices in risk management meetings or solicit their input on additional risks the program should have been tracking as a result of the business system deficiencies, such as unreliable contractor data, as previously mentioned.

Ensuring programs track risks raised by stakeholders. We found two instances when programs did not include risks raised by stakeholders, either in program documents or during meetings, in their risk registers.

- In May and June of 2021, stakeholders conducted two program assessments for the selected Cybersecurity and Infrastructure Security Agency program as it prepared for an acquisition decision event. These stakeholders identified several sources of technical risk in these assessments, including insufficient cybersecurity planning and analysis, incomplete technical planning, and risks following the introduction of new capabilities. Program officials stated that the program did not fully incorporate these stakeholder-identified risks into the risk register prior to, or immediately after, the program's acquisition decision event meeting. Contrary to DHS PARM's risk management guidance, program officials explained that they did not include all of the stakeholder-identified risks in their risk register because stakeholders and leadership can review these assessments separately. However, the information in these assessments remains static until programs incorporate it into the risk register where the risks can be tracked and updated.

- During the selected Coast Guard program's March 2022 pre-Acquisition Review Board meeting, a senior Navy official raised concerns about the program's aggressive construction schedule. However, the program did not add the risk to its register or communicate the risk in the briefing material when the program requested approval for an early production phase in May 2022. Program officials stated that they did not add the overall schedule risk into the risk register because they had already added more specific schedule risks, such as those related to workforce and supply chain, to the risk register. However, by not tracking the program's overall schedule risk, the program did not consistently communicate this risk to leadership or analyze the consequences of the risk, such as effects on the *Polar Star*'s service life extension program.[32]

While DHS acquisition policy and guidance embed stakeholder engagement throughout the acquisition process, DHS PARM's risk management guidance does not describe how programs should consistently incorporate and document stakeholder input. Specifically, it provides minimal information on how programs should document stakeholder engagement on acquisition risk management as found in leading practices. The guidance also does not include how to manage stakeholder coordination, such as through a stakeholder engagement plan or stakeholder register, and provides minimal direction on how to document stakeholder input in the risk register.

Further, the guidance does not provide a comprehensive list of key acquisition documents, relevant meetings, or other forums that programs should consult for risks identified by stakeholders. The guidance states that risks documented in key acquisition documents should be included in the risk register and managed. While the guidance notes some key acquisition documents that programs can consult for risks, this list does not comprehensively reference the required documents outlined in DHS acquisition policy. For example, it does not mention the cost estimating baseline document, which describes the basic technical, programmatic,

[32]In 2018, we also raised concerns about the program's aggressive schedule and recommended that the program set realistic schedule goals for its three ships before the option for construction of the lead ship was awarded. The Coast Guard concurred with the recommendation, but the program awarded the contract for design and construction of the lead ship in 2019 and the option for construction of the second ship in 2021 without developing a realistic schedule in accordance with best practices for project schedules. We closed this recommendation as not implemented. See GAO-18-600. In July 2023, we found that the program had yet to establish a realistic schedule. See GAO, *Coast Guard Acquisitions: Polar Security Cutter Needs to Stabilize Design Before Starting Construction and Improve Schedule Oversight,* GAO-23-105949 (Washington, D.C.: July 27, 2023).

and operational characteristics of a program and helps identify risks that can significantly affect the life-cycle costs. Further, DHS PARM's guidance does not include other information that could assist programs in ensuring stakeholder input is incorporated, such as the corresponding stakeholders who assist with each type of document and the types of risks these stakeholders have expertise in. The guidance also does not emphasize that programs should incorporate risks identified by stakeholders during key meetings, such as the pre-Acquisition Review Board briefings, into the risk register.

In contrast, we found an example of component-level guidance that included additional details on sources of stakeholder inputs. The Cybersecurity and Infrastructure Security Agency's risk management guidance provides tables for each phase of the program life cycle that include relevant key acquisition documents, their associated risk inputs, and in some cases, the responsible stakeholder. For example, the guidance notes that prior to acquisition decision event 2A—which authorizes a program to enter into the obtain phase of the life cycle—programs should submit a test and evaluation master plan. The plan documents the testing risks and approach to managing cybersecurity risks.

Further, DHS PARM's guidance states programs should include all risks identified by stakeholders in acquisition documents. However, officials from several DHS-level stakeholder offices shared that programs should decide which stakeholder-identified risks to include in the risk register. For example, one official from the Office of the Chief Procurement Officer shared that they were not aware of any guidance on how to incorporate contracting risks from a program's acquisition plan into the risk register. Officials from the Cost Analysis Division stated that programs have discretion on whether to include risks identified in the life-cycle cost estimate into the risk register. An official from the Science and Technology Directorate said that their office can provide potential sources of technical risks in their technical assessments, but that programs have discretion in identifying risks they want to include.

DHS PARM officials stated that they plan to include additional guidance on stakeholder engagement in the fall 2023 update to the risk management guidance. According to these officials, proposed changes may include a recommendation that programs hold stakeholder interviews to help identify areas of concern and consideration for risks. Additionally, officials plan to add information about risks identified in program assessments. However, it is too early to know if these planned revisions

will address the gaps we identified in DHS PARM's risk management guidance. Ensuring that planned updates to DHS PARM's guidance reflect leading principles for soliciting and documenting stakeholder input throughout the risk management process can help programs reduce optimistic biases. This is important because optimism bias can lead to an underestimation of risks, and potentially worse program outcomes. Similarly, ensuring the updated guidance includes a more comprehensive list of sources for stakeholder inputs will help programs consider and incorporate all stakeholder-identified risks.

Selected Programs Did Not Always Communicate Current Risk Information to DHS Leadership

DHS PARM risk management guidance and program risk management approaches do not fully reflect leading practices related to communicating information to leadership. Leading principles that we and the Project Management Institute have identified emphasize the importance of communication with leadership to accomplish common program goals.[33] Federal internal control standards further state that agencies should design control activities to achieve goals and respond to risks, including accurate and timely records.[34] Such control activities could include guidance that facilitates programs communicating up-to-date risk information to leadership, such as when programs plan to take risk mitigation steps. This helps to ensure leadership can provide input or make relevant decisions in a timely manner.

Several programs we reviewed did not always communicate up-to-date risk information to DHS and component leadership. Specifically, programs did not report on the most up-to-date risks in their Acquisition Review Board briefings or consistently provide current dates on when programs plan to complete actions in response to risks in their risk registers.

Officials from four programs we reviewed shared that there is a lag between the date of the risk register used to prepare the briefing slides and the date of the Acquisition Review Board meeting. These briefing slides need to go through several layers of review and approval, which results in lag time. According to program officials, the lag can be anywhere from 4 to 12 weeks, and during this time, risks may have changed and additional risks may have emerged. Some program officials

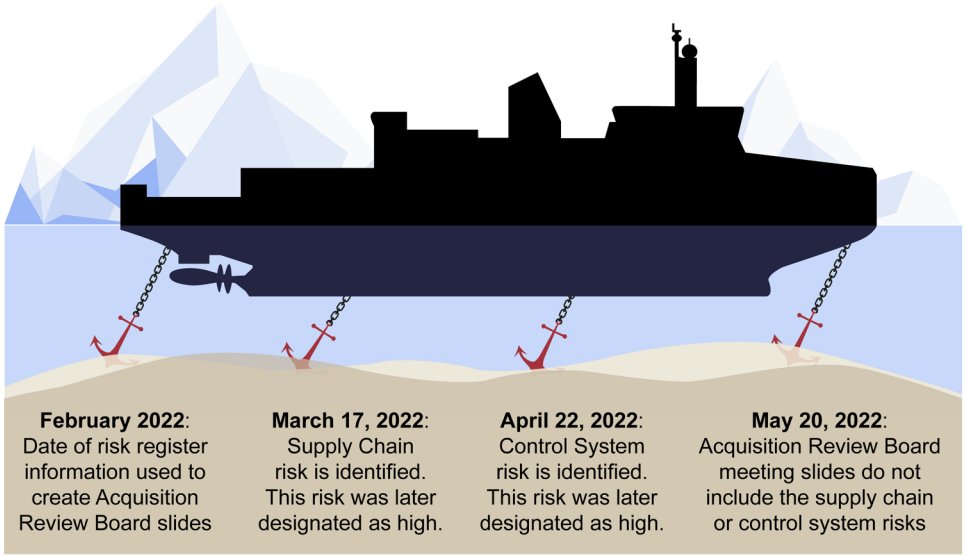
[33]GAO-17-63. Project Management Institute, Inc., *A Guide to the Project Management Body of Knowledge (PMBOK® Guide),* Sixth Edition (2017); and Project Management Institute, Inc., *The Standard for Portfolio Management*, Fourth Edition (2017).

[34]GAO-14-704G.

stated that they can verbally communicate any newly identified risks during the briefing.

However, our analysis of program documents found the lag of the risk information in the briefing slides increases the possibility of programs not communicating high risks to leadership. For example, in its May 2022 Acquisition Review Board briefing slides, the selected Coast Guard program did not include two high risks that it identified in March and April 2022 and tracked in its risk register. Program officials explained that they did not have sufficient time to update the slides before the required reviews. The briefing slides also did not disclose that the risk information included was as-of February 2022. While program officials stated that they verbally discussed a supply chain risk during the meeting, there was no significant discussion of a risk related to control systems (see fig. 5).

Figure 5: Lag Time in a Selected Coast Guard Program's Risks Presented to Department of Homeland Security Leadership



Source: Bollinger Mississippi Shipbuilding and GAO analysis of Coast Guard information and interviews; GAO (ship). | GAO-23-106249

We additionally found inconsistencies in how programs maintain the estimated completion date for risk mitigation steps. The selected CBP program did not update its estimated completion dates for its risk responses once those dates had elapsed. Program officials stated they treated the initial estimated completion date as a baseline for internal tracking, which is consistent with what DHS PARM officials told us

programs should do. Yet, officials from the selected Cybersecurity and Infrastructure Security Agency program shared that sometimes they retain the original estimated completion date but other times will update the date. Further, several of the other programs we selected for review shared that they do update the estimated completion date in the risk register to reflect revised time frames.

DHS PARM's risk management guidance states that the purpose of risk reporting is to ensure management receives all necessary information to make timely and effective decisions. Additionally, it prompts programs to include estimated completion dates in risk registers and on Acquisition Review Board briefing materials. Yet, the guidance does not:

- Fully convey how a program should communicate the currency of risk information to leadership in Acquisition Review Board meetings. This may include encouraging verbal communication of newly identified risks and including the as-of date on risk slides.
- Specify how programs should handle updates to the estimated completion dates of actions taken in response to risks once the planned date has elapsed. While programs primarily use risk registers as a working-level tool to manage risks, stakeholders and agency leadership also review the registers for insight. Information on revised estimated completion dates could be of relevance to their understanding of the risk's current status. Further, documenting these dates in a consistent manner could help ensure risk registers serve as effective repositories and provide traceability for programs.

Without additional guidance on communicating the currency of risk information, DHS leadership cannot be sure they have the most up-to-date risk information from programs during Acquisition Review Board briefings. They also may not have the information necessary to prompt questions about newly identified risks during these briefings. Further, without additional guidance on consistently documenting estimated completion dates, programs may not be providing leadership and stakeholders with timely visibility into how they are managing risks.

Conclusions

In recent years, DHS has recognized the importance of acquisition risk management by strengthening its related guidance and approaches. DHS's risk management guidance reflects certain leading principles that we and others identified, which provide programs with a solid foundation for managing their risks. However, DHS can go further in helping programs guard against underestimating and missing risks by providing

steps for improving the objectivity of risk assessments and managing realized risks.

DHS has also shown a commitment to taking a portfolio management approach to its acquisition programs. As DHS continues to emphasize the importance of adopting risk management tenets, it should provide its portfolio managers with direction on conducting portfolio risk management. This could help optimize decision-making at the portfolio-level, rather than relying on individual ad hoc decisions by programs and portfolio managers.

Additionally, DHS faces an inherent tension between providing programs with flexibility in their risk management approaches and implementing a DHS-wide repository that captures the knowledge necessary to efficiently share risk data, learn from past mistakes, and manage risks at the portfolio-level. However, until DHS weighs the benefits and drawbacks of implementing such a risk repository, institutional knowledge gained by programs are more likely to remain siloed and untapped.

Finally, DHS designed an acquisition framework that values communication with stakeholders and leadership about risks—a key ingredient for cultivating a culture in which risks can be robustly discussed and considered before programs move forward. However, DHS can further ensure stakeholders' voices—critical checks on a program's optimistic biases—are heard by better documenting their inputs and providing a comprehensive one-stop-shop of acquisition documents with stakeholder-identified risks. DHS can also improve its guidance to help ensure acquisition leaders receive the most current information on a program's top risks and related management steps before authorizing a program to move forward. As DHS plans to update its acquisition risk management guidance in fall 2023, the department has an opportunity to expand its programs' toolkit for managing risks and improve their chances of meeting cost, schedule, and performance goals.

Recommendations for Executive Action

We are making eight recommendations to the Department of Homeland Security:

The Secretary of Homeland Security should ensure that when the Office of Program Accountability and Risk Management updates its risk management guidance, that it include methods for improving the objectivity of risk assessments. (Recommendation 1)

The Secretary of Homeland Security should ensure that when the Office of Program Accountability and Risk Management updates its risk management guidance, that it include additional direction on managing realized risks, such as how to manage the consequences of realized risks and how to identify additional risks that may result from realized risks. (Recommendation 2)

The Secretary of Homeland Security should ensure that when the Office of Program Accountability and Risk Management updates its risk management guidance, that it include leading principles on portfolio-level risk management. (Recommendation 3)

The Secretary of Homeland Security should ensure that the Office of Program Accountability and Risk Management (1) assesses the costs and benefits of developing or acquiring the capability to systematically share risk management knowledge, such as data in risk registers and risk management approaches, across the department, and (2) determines whether to implement such a capability. (Recommendation 4)

The Secretary of Homeland Security should ensure that when the Office of Program Accountability and Risk Management updates its risk management guidance, that it further incorporate leading practices for documenting engagement with stakeholders, such as ways to identify the appropriate stakeholders to involve and what input stakeholders have provided on risks. (Recommendation 5)

The Secretary of Homeland Security should ensure that when the Office of Program Accountability and Risk Management updates its risk management guidance, that it clarifies how programs should include risks raised in required acquisition documents and relevant meetings, such as by providing a more comprehensive list of required acquisition documents and forums where stakeholder risks are identified, to ensure these risks are consistently accounted for in risk registers. (Recommendation 6)

The Secretary of Homeland Security should ensure that when the Office of Program Accountability and Risk Management updates its risk management guidance for briefing the Acquisition Review Board on risks, that it (1) include additional direction on including as-of dates for risk information, and (2) clarify how programs should communicate on risks that have arisen or changed since the as-of date. (Recommendation 7)

The Secretary of Homeland Security should ensure that when the Office of Program Accountability and Risk Management updates its risk

management guidance, it include additional direction on maintaining up-to-date estimated completion dates for risk mitigation steps. (Recommendation 8)

Agency Comments

We provided a draft of this report to DHS for review and comment. In its written comments (reproduced in appendix III), DHS concurred with all eight of our recommendations and described its plans to address them. DHS also provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees and the Secretary of Homeland Security. 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 me at (202) 512-4841 or makm@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.

Marie A. Mak
Director, Contracting and National Security Acquisitions

Appendix I: Objectives, Scope, and Methodology

This report assesses the extent to which the Department of Homeland Security (DHS) has (1) addressed acquisition risk management principles at the program and portfolio levels, (2) shared information to facilitate acquisition risk management, and (3) involved stakeholders and leadership in acquisition risk management. This report focuses on acquisition risk management for DHS major acquisition programs. Major acquisition programs are those with life-cycle costs of $300 million or more.[1] Acquisition risk management refers to the process of managing potential negative effects on a program's cost, schedule, and performance relative to its plan.

To conduct our work, we reviewed acquisition risk management policies and guidance from DHS's Office of Program Accountability and Risk Management (PARM)—the office responsible for DHS's overall acquisition governance process. The DHS acquisition policies refer to DHS's acquisition management directive and instruction.[2] The DHS PARM acquisition risk management guidance refers to an October 2018 risk management guide, training, and templates for how programs track risks and present risks to the DHS Acquisition Review Board at acquisition decision events.[3]

To address our first objective, we evaluated DHS PARM's acquisition risk management guidance to determine the extent which it included six leading principles for acquisition risk management at both the program and portfolio level: planning for, identifying, assessing, responding to, monitoring, and communicating risks. We identified these six leading principles based on a review of three sources: (1) the Project Management Institute's *A Guide to the Project Management Body of Knowledge (PMBOK® Guide),* Sixth Edition; (2) the Project Management

[1]DHS defines major acquisition programs as those with life-cycle cost estimates of $300 million or more. In some cases, DHS may define a program with a life-cycle cost estimate less than $300 million as a major acquisition if it has significant strategic or policy implications for homeland security, among other things.

[2]DHS Directive 102-01, *Acquisition Management Directive* (July 28, 2015) (incorporating change 1, Feb. 25, 2019); DHS Instruction 102-01-001, Revision 02, *Acquisition Management Instruction* (Jan. 10, 2023).

[3]DHS Office of Program Accountability and Risk Management, *Risk Management Training Aide for Acquisition Programs* (Oct. 9, 2018).

Institute's *The Standard for Portfolio Management,* Fourth Edition; and (3) GAO's leading principles for enterprise risk management.[4] Specifically:

- *A Guide to the Project Management Body of Knowledge* identifies seven processes for project risk management: planning, identification, qualitative analysis, quantitative analysis, response planning, response implementation, and monitoring. For the purposes of our analysis, we combined the two processes of qualitative analysis and quantitative analysis into one step—assessing risk. We also combined the two processes of response planning and response implementation into one step—responding to risk. *A Guide to the Project Management Body of Knowledge* does not include a separate process for communication. However, the guide includes communication principles as part of the monitoring step. For the purposes of our analysis, we included a separate step for communicating risks.
- The *Standard for Portfolio Management* identifies four key elements in portfolio risk management: planning, identification, analysis, and response. The standard does not include separate elements for monitoring and communicating risks. However, the standard includes monitoring and communication principles throughout the four elements.
- GAO's leading practices for enterprise risk management identify six essential elements for managing enterprise risks: aligning risk management processes to agency goals, identifying risks, assessing risks, selecting risk responses, monitoring risks, and communicating and reporting on risks. Acquisition risks and enterprise risks are not synonymous, but certain enterprise risk management principles can be applied to acquisition risk management.

We compared and synthesized the three sources above to identify the six principles for acquisition risk management.

We also determined that the control activities component of internal controls was significant to the first objective, along with the principle that management should implement control activities by documenting through policies how the agency will achieve its goals. We assessed DHS's efforts to implement control activities through development of policies for two risk

[4]Project Management Institute, Inc., *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)*, Sixth Edition (2017); Project Management Institute, Inc., *The Standard for Portfolio Management*, Fourth Edition (2017). GAO, *Enterprise Risk Management: Selected Agencies' Experiences Illustrate Good Practices in Managing Risk,* GAO-17-63 (Washington, D.C.: Dec. 1, 2016). *PMBOK* is a trademark of Project Management Institute, Inc.

management objectives identified by DHS: (1) objectively assessing risks, and (2) managing realized risks.

To inform our work, we also reviewed acquisition risk management policies and guidance from the DHS components that manage major acquisition programs to identify variations across components. As of October 2022, eight components managed major acquisition programs:

- Countering Weapons of Mass Destruction Office,
- Cybersecurity and Infrastructure Security Agency,
- Federal Emergency Management Agency (FEMA),
- Management Directorate,[5]
- Science and Technology Directorate,[6]
- Transportation Security Administration (TSA),
- U.S. Coast Guard, and
- U.S. Customs and Border Protection (CBP).

To address our second objective, we reviewed how DHS and the components shared risk management information across components and programs through data and document repositories and working groups. We compared these efforts to leading practices for lessons

[5]In addition to acquiring major acquisition programs, the Management Directorate is also a support component. The directorate provides assistance and guidance to other DHS components and external organizations and includes functions like budget, finance, information technology, facilities, human capital, and acquisitions.

[6]As of October 2022, the Science and Technology directorate was acquiring one major acquisition program—a facility construction project. As of January 2023, the directorate's one program had achieved initial operational capability and was no longer designated as a major acquisition program. For the purposes of our review, we included the Science and Technology Directorate as one of the eight DHS components that acquired major acquisition programs.

learned identified in prior GAO work, including practices related to storing and sharing information.[7]

To address our third objective, we evaluated DHS PARM's acquisition risk management guidance against one of the leading principles—communication—which was the most relevant leading principle related to involving stakeholders and leadership. Within the communication leading principle, we identified leading practices related to stakeholder engagement and documentation of stakeholder input based on a review of the three sources previously noted: (1) the Project Management Institute's *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)*, Sixth Edition; (2) the Project Management Institute's *The Standard for Portfolio Management*, Fourth Edition; and (3) GAO's leading practices for enterprise risk management.[8]

We also determined that the control activities component of internal controls was significant to the third objective, along with the principle that management should design control activities to achieve goals and respond to risks. We assessed DHS's efforts to design control activities—specifically, accurate and timely records—for two types of records. First, we assessed the timeliness of risk information presented in program briefings to DHS leadership at Acquisition Review Boards meetings. We compared the as-of dates of the briefings to the as-of dates of the risk registers used to develop the briefings to determine any lag times. Second, we assessed the consistency of estimated completion dates reported by programs for actions in response to risks tracked in program risk registers.

To provide illustrative examples of how DHS implemented risk management approaches for all three objectives, we selected a nongeneralizable sample of five major acquisition programs with investment decision events between May 2020 (1 year after DHS revised

[7]GAO, *Grants Management: OMB Should Collect and Share Lessons Learned from Use of COVID-19-Related Grant Flexibilities*, GAO-21-318 (Washington, D.C.: Mar. 31, 2021); *DOD Utilities Privatization: Improved Data Collection and Lessons Learned Archive Could Help Reduce Time to Award Contracts*, GAO-20-104 (Washington, D.C.: Apr. 2, 2020); *Project Management: DOE and NNSA Should Improve Their Lessons-Learned Process for Capital Asset Projects*, GAO-19-25 (Washington, D.C.: Dec. 21, 2018); and *Federal Real Property Security: Interagency Security Committee Should Implement a Lessons-Learned Process*, GAO-12-901 (Washington, D.C.: Sept. 10, 2012).

[8]GAO-17-63. Project Management Institute, Inc., *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)*, Sixth Edition (2017); and Project Management Institute, Inc., *The Standard for Portfolio Management*, Fourth Edition (2017).

its acquisition risk management policies) and November 2022. We then selected based on the following criteria:

- Representation of DHS components;
- Mix of non-IT and IT programs;
- Mix of investment decision events, which included acquisition decision events, rebaseline decisions, and authorization of resources;
- Mix of programs that experienced successes or challenges with risk management identified by us or DHS, which we verified through program documents; and
- Programs with potential interdependencies with other programs.

See table 3 for the programs we selected.

Table 3: Selected DHS Major Acquisition Programs

Component	Program	Description	Investment decision event	Selected characteristics
Cybersecurity and Infrastructure Security Agency	Next Generation Network Priority Services Phase 2	The program will provide data and video services to key government personnel during emergencies.	July 2021 acquisition decision event 2A	IT Experienced successes with risk management Potential interdependencies with Next Generation Network Priority Services Phase 1
Federal Emergency Management Agency (FEMA)	Grants Management Modernization	The program is working to develop a new IT system that aims to streamline, consolidate, and modernize FEMA's grant management process across over 40 active grant programs.	Jan. 2021 rebaseline	IT Experienced successes with risk management
Transportation Security Administration	Credential Authentication Technology	The program creates units used to verify and validate passenger identification and flight information prior to entering secure areas in airports.	June 2022 rebaseline	IT No information on risk management approach prior to GAO review

Component	Program	Description	Investment decision event	Selected characteristics
U.S. Coast Guard	Polar Security Cutter	The program consists of three yet-to-be-built ships that will have specialized hulls that can break through polar ice and assist the U.S. in maintaining access to the Arctic and Antarctic polar regions.	June 2022 authorization of an early production phase	Non-IT Experienced challenges with risk management Potential interdependencies with *Polar Star* service life extension program
U.S. Customs and Border Protection	Non-Intrusive Inspection Integration	The program is aimed at integrating—through CBP's network—non-intrusive units of varying sizes that scan, detect, and prevent illicit entry and exit of contraband in a nondestructive way.	Nov. 2022 acquisition decision event 2A	Both IT and non-IT Experienced successes with risk management Potential interdependencies with Non-Intrusive Inspection Systems

Source: GAO analysis of Department of Homeland Security (DHS) information. | GAO-23-106249

For each program, we reviewed acquisition documents and interviewed program officials.

To supplement our analysis, in addition to our sample of five programs, we also reviewed information from other DHS major acquisition programs obtained through prior and ongoing GAO reviews, as well as from DHS PARM and component officials. These programs included CBP's Biometric Entry-Exit program, FEMA's Enterprise Data and Analytics Modernization Initiative program, and the Management Directorate's Homeland Advanced Recognition Technology and Financial Systems Modernization programs.

Additionally, we interviewed officials from DHS PARM, each of the eight components with major acquisition programs, and selected DHS lines of business offices, including DHS's Office of the Chief Financial Officer, Cost Analysis Division; Office of the Chief Procurement Officer; and the Science and Technology Directorate, including the Test and Evaluation Division.[9]

[9]In addition to acquiring major acquisition programs as a component, the Science and Technology Directorate also serves as a support component by providing inputs on technical risks for major acquisition programs.

We conducted this performance audit from September 2022 to August 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Summary of Department of Homeland Security Components' Risk Management Guidance

Table 4: Acquisition Risk Management Guidance of Department of Homeland Security (DHS) Components

DHS component	Supplemental risk management guidance
Coast Guard	Standard operating procedures direct programs to establish a risk management team and to organize identified risks by a work breakdown structure to ensure all program elements are considered Standard operating procedures provide general areas that should be considered during risk identification efforts, such as immature or obsolete products and technologies, engineering change orders, and contractors and subcontractor management
Countering Weapons of Mass Destruction Office	Guidebook provides information on realized risks and opportunity management, in addition to risk management. Realized risks are risks that have occurred. Opportunities are events or conditions that can have a positive effect on the program
Customs and Border Protection (CBP)	Directive emphasizes risk tolerance and implementing management practices that reward innovation Directive notes that the Component Acquisition Executive designates a CBP Chief Risk Officer, who is responsible for establishing risk tolerance procedures and guiding programs to encourage risk taking and reward innovation, among other responsibilities
Cybersecurity and Infrastructure Security Agency	Guidebook provides step-by-step risk management instructions for programs, including characteristics of successful risk management approaches and detailed instructions for reviewing risk response plans Templates for managing stakeholder engagement to encourage programs to track relevant stakeholders in a register, assess upfront the extent that stakeholders will be involved in the program, and establish preferred communication channels
Federal Emergency Management Agency	None: uses DHS guidance
Management Directorate	None: uses DHS guidance
Science and Technology Directorate	None: uses DHS guidance
Transportation Security Administration	Acquisition manual contains some information on managing risks, including instructions for documenting risk management processes in risk management plans and risks in risk registers Template for executive program review meetings—during which programs inform leadership and other stakeholders of program updates—includes status updates on risks

Source: GAO analysis of information from Coast Guard, Countering Weapons of Mass Destruction Office, Customs and Border Protection, Cybersecurity and Infrastructure Security Agency, Federal Emergency Management Agency, Management Directorate, Science and Technology Directorate, and Transportation Security Administration. | GAO-23-106249

Appendix III: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

August 8, 2023

Marie A. Mak
Director, Contracting and National Security Acquisitions
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

Re: Management Response to Draft Report GAO-23-106249, "DHS ACQUISITIONS: Opportunities Exist to Enhance Risk Management"

Dear Ms. Mak:

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS or the Department) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

DHS leadership is pleased to note GAO's positive recognition that the Department's risk management guidance broadly reflects the six leading principles of acquisition risk management identified by GAO at the program level, and that the guidance encourages programs to engage with stakeholders and leadership throughout the acquisition lifecycle. GAO also noted that DHS designed an acquisition framework that values communication with stakeholders and leadership about risks—which is a key component in cultivating a culture in which risks can be robustly discussed and considered before programs move forward. DHS remains committed to following sound program management practices in the acquisition lifecycle, and in developing and delivering capabilities to end users.

The draft report contained eight recommendations with which the Department concurs. Enclosed find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for GAO's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H CRUMPACKER Digitally signed by JIM H CRUMPACKER Date: 2023.08.08 12:09:46 -04'00'

JIM H. CRUMPACKER, CIA, CIE
Director
Departmental GAO-OIG Liaison Office

Enclosure

Enclosure: Management Response to Recommendations Contained in GAO-23-106249

GAO recommended that the Secretary of Homeland Security:

Recommendation 1: Ensure that when the Office of Program Accountability and Risk Management updates its risk management guidance, that it include methods for improving the objectivity of risk assessments.

Response: Concur. The Management Directorate's Office of Program Accountability and Risk Management (PARM) is in the process of updating its risk management guidance, to include methods for improving objectivity of risk assessments in the next revision, as appropriate. PARM programmatic risk guidance documents include, but are not limited to: (1) the Risk Management Training Aide for Acquisition Programs," dated October 9, 2018, (2) risk training; and (3) Acquisition Review Board (ARB) risk slide templates, etc. Estimated Completion Date (ECD): January 31, 2024.

Recommendation 2: Ensure that when the Office of Program Accountability and Risk Management updates its risk management guidance, that it include additional direction on managing realized risks, such as how to manage the consequences of realized risks and how to identify additional risks that may result from realized risks.

Response: Concur. As part of updating its risk management guidance PARM will include additional direction on managing realized risks, to include how to manage the consequences of realized risks and how to identify additional risks that may result from realized risks. ECD: January 31, 2024.

Recommendation 3: Ensure that when the Office of Program Accountability and Risk Management updates its risk management guidance, that it include leading principles on portfolio-level risk management.

Response: Concur. As part of updating its risk management guidance PARM will include leading principles on portfolio-level risk management. ECD: January 31, 2024.

Recommendation 4: Ensure that the Office of Program Accountability and Risk Management (1) assesses the cost and benefits of developing or acquiring the capability to systematically share risk management knowledge, such as data in risk registers and risk management approaches, across the department and (2) determines whether to implement such a capability.

Response: Concur. PARM will assess costs and benefits of developing, or acquiring, a capability to systematically share risk management knowledge across the department, such as data in risk registers and risk management approaches. Following this assessment, PARM

2

will then determine whether to implement a capability, as appropriate. ECD: July 31, 2024.

Recommendation 5: Ensure that when the Office of Program Accountability and Risk Management updates its risk management guidance that it further incorporate leading practices for documenting engagement with stakeholders, such as ways to identify the appropriate stakeholders to involve and what input stakeholders have provided on risks.

Response: Concur. As part of updating its risk management guidance PARM will further incorporate leading practices for documenting engagement with stakeholders, such as ways to identify the appropriate stakeholders to involve and what input stakeholders have provided on risks. ECD: January 31, 2024.

Recommendation 6: Ensure that when the Office of Program Accountability and Risk Management updates its risk management guidance it clarifies how programs should include risks raised in required acquisition documents and relevant meetings, such as by providing a comprehensive list of required acquisition documents and forums where stakeholder risks are identified, to ensure these risks are consistently accounted for in risk registers.

Response: Concur. As part of updating the risk management guidance PARM will: (1) add to the document examples listed in the "Risk Management Training Aide for Acquisition Programs," dated October 9, 2018; and (2) reference DHS Instruction 102-01-001, Revision 02 "Acquisition Management," dated January 10, 2023, for other documents. ECD: January 31, 2024.

Recommendation 7: Ensure that when the Office of Program Accountability and Risk Management updates its risk management guidance for briefing the Acquisition Review Board on risks that it (1) includes additional direction on including as-of dates for risk information, and (2) clarify how programs should communicate on risks that have arisen or changed since the as-of date.

Response: Concur. As part of updating the risk management guidance PARM will highlight communication of risks that have arisen or changed since the as-of date in ARB presentations. The update will include what risk information needs to be communicated, to whom it needs to be communicated (stakeholders), and when it needs to be communicated. PARM will update risk management guidance to ensure risk information is current and reflected in the ARB presentations. ECD: January 31, 2024.

Recommendation 8: Ensure that when the Office of Program Accountability and Risk Management updates its risk management guidance, it includes additional direction on maintaining up-to-date estimated completion dates for risk mitigation steps.

Response: Concur. As part of updating the risk management guidance PARM will update and expand guidance on maintaining up-to-date estimated completion dates for risk mitigation steps. ECD: January 31, 2024.

3

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Marie A. Mak, (202) 512-4841 or makm@gao.gov

Staff Acknowledgments

In addition to the contact named above, the following staff members made key contributions to this report: Meghan Perez (Assistant Director), Claire Li (Analyst-in-Charge), Shelby Clark, Lorraine Ettaro, Lori Fields, Laura Greifner, Kelly Rolfes-Haase, and Anne Louise Taylor.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

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

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

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

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

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

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

Congressional Relations

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

Public Affairs

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

Strategic Planning and External Liaison

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