U.S. GOVERNMENT ACCOUNTABILITY OFFICE

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

**Comptroller General**
**of the United States**

Accessible Version

August 19, 2024

The Honorable Alejandro Mayorkas
Secretary of Homeland Security
Washington, D.C. 20528

**Priority Open Recommendations: Department of Homeland Security**

Dear Secretary Mayorkas:

The purpose of this letter is to update you on the overall status of the Department of Homeland Security's (DHS) implementation of GAO's recommendations and to call your continued personal attention to areas where open recommendations should be given high priority.[1] In November 2023, we reported that, on a government-wide basis, 75 percent of our recommendations made 4 years ago were implemented.[2] DHS's recommendation implementation rate was 84 percent. As of June 2024, DHS had 478 open recommendations. Fully implementing these open recommendations could significantly improve agency operations.

Since our June 2023 letter, DHS has implemented 16 of our 42 open priority recommendations.

- In 2023, the Federal Emergency Management Agency (FEMA) implemented procedures to annually analyze the profit Write Your Own (WYO) insurers earn and the related compensation received and expenses incurred to sell and service federal flood insurance policies and adjust and pay claims. Annually analyzing actual WYO expenses, compensation payments, and resulting profit are now part of FEMA's established business processes with defined roles for its Federal Insurance and Mitigation Administration staff. These procedures and the insights gained from analysis of the

[1]Priority recommendations are those that GAO believes warrant priority attention from heads of key departments or agencies. They are highlighted because, upon implementation, they may significantly improve government operations, for example, by realizing large dollar savings; eliminating mismanagement, fraud, and abuse; or making progress toward addressing a high-risk or duplication issue.

[2]GAO, *Performance and Accountability Report: Fiscal Year 2023*, GAO-24-900483 (Washington, D.C.: Nov. 15, 2023).

results each year will help to inform FEMA as it revises its compensation practices for WYO insurers as required by the Biggert-Waters Flood Insurance Reform Act of 2012.[3]

- FEMA took steps to assess how effectively its disaster workforce was deployed to meet mission needs in the field. Specifically, FEMA included questions in its 2023 National Collection Analysis Priorities quarterly survey to collect perspectives on how well deployed staff met response needs. The agency began collecting data using the survey in January 2023. According to FEMA officials, the data will be used to help inform after-action reviews and deployment decisions. These actions should help FEMA headquarters officials assess whether its deployment strategies effectively met mission needs and to take corrective actions, if necessary.[4]

- FEMA took several actions to address the management of federal resources for future incidents.[5] In 2021, FEMA developed the National Framework for Allocation of Constrained Public Health Resources. It establishes a methodology to address constrained federal resources when a public health incident arises. In November 2023, FEMA reported that the U.S. Department of Health and Human Services (HHS) is the executive agent for all actions associated with the National Strategy for a Resilient Public Health Supply Chain and will house the framework.[6] As a result, the federal government should be better positioned to respond and address resource issues in future public health incidents.

- FEMA took steps to address two recommendations on the mandatory purchase requirement of the National Flood Insurance Program, which we made in July 2021.[7] As of December 2023, FEMA completed its draft evaluation of flood risk data and recommended possible uses of flood risk information to inform potential changes to the mandatory purchase requirement. In April 2024, it provided the report to Congress. FEMA also determined what information to incorporate—both internally and externally—related to the mandatory purchase requirement, and used it to develop strategies for increasing consumer participation in the flood insurance market.

By addressing these recommendations, FEMA has provided information to Congress to help inform its decision making on how, if at all, to revise the mandatory purchase requirement and improve the ability of the requirement to increase consumer participation and reduce future federal disaster assistance expenditures. FEMA has also begun to better

---

[3]GAO, *Flood Insurance: Opportunities Exist to Improve Oversight of the WYO Program*, GAO-09-455 (Washington, D.C.: August 21, 2009).

[4]GAO, *FEMA Disaster Workforce: Actions Needed to Address Deployment and Staff Development Challenges*, GAO-20-360 (Washington, D.C.: May 4, 2020).

[5]GAO, *COVID-19: Federal Efforts Could Be Strengthened by Timely and Concerted Action*, GAO-20-701 (Washington, D.C.: September 21, 2020).

[6]The Department of Health and Human Services established an Administration for Strategic Preparedness and Response that will house the framework and all other documents finalized as part of the combined effort.

[7]GAO, *National Flood Insurance Program: Congress Should Consider Updating the Mandatory Purchase Requirement*, GAO-21-578 (Washington, D.C.: July 30, 2021).

target its outreach to communities, lenders, property owners, and other stakeholders to increase consumer participation in the flood insurance market.

- FEMA took steps to designate a lead entity with responsibility for providing oversight of agency-wide efforts to manage fraud risks to Public Assistance (PA) emergency work grants. In August 2023, FEMA provided a copy of its updated directive for fraud prevention and investigation in FEMA programs. This directive outlines the Office of Chief Security Officer's Fraud Investigations and Inspections Division's (FIID) responsibilities for managing and coordinating agency-wide efforts to prevent, detect, deter, investigate, and report fraud, waste, and abuse. Designating a lead entity for fraud risk management efforts and documenting these responsibilities will help ensure that FEMA is managing its fraud risks and that its efforts address areas most at risk for fraud in PA emergency work grants.[8]

- DHS took steps to address two recommendations related to its processing of family members at the southwest border. DHS identified and communicated the information that its components need in order to process family members who are apprehended together.[9] U.S. Customs and Border Protection (CBP), in coordination with the Office of Immigration Statistics, issued a memorandum in April 2023 with updated, agency-wide guidance on recording, linking, and processing family groups. As a result, DHS should have greater assurance that its components are identifying all individuals who may be eligible for relief from removal from the U.S. based on their family relationships.

  In addition, DHS evaluated options for developing a unique identifier shared across components' data systems to link family members apprehended together, as we recommended. As of 2023, CBP uses these identifiers in its data systems and makes them available to other DHS components through a shared portal. Developing and sharing these identifiers should help bridge component information gaps about family members CBP apprehends.

- CBP took steps to enable the drawback claim[10] targeting feature in the Automated Commercial Environment (ACE)[11] and to target drawback claims for review that were accepted into ACE when the claim targeting feature was disabled. For drawback claims that were submitted when the claim targeting feature in ACE was disabled, CBP reviewed claims on an ongoing basis and estimated that it denied $163,370,381 (or $164,691,014 in fiscal year 2023 dollars using a net present value calculation) in improper refunds as a

---

[8]GAO, *Disaster Assistance: FEMA Should Take Additional Actions to Strengthen Fraud Risk Management for Public Assistance Emergency Work Grants*, GAO-20-604 (Washington, D.C.: September 29, 2020).

[9]GAO, *Southwest Border: Actions Needed to Address Fragmentation in DHS's Processes for Apprehended Family Members*, GAO-20-274 (Washington, D.C.: February 19, 2020.)

[10]Through the drawback program, CBP refunds up to 99 percent of duties, taxes, or fees previously paid by an importer. CBP makes these refunds on imported goods on which the importer previously paid duties, taxes, or fees, and subsequently exported from the U.S. or destroyed.

[11]CBP designated ACE as the electronic system for filing drawback claims. ACE is programmed to target certain drawback claims for CBP's review. When CBP transitioned the drawback program to ACE starting on February 24, 2018, a system error forced CBP to disable the claim targeting feature in ACE, according to CBP officials.

result of these reviews. In addition, as of February 2023, CBP enabled the claim targeting feature in ACE to randomly target claims for review. In March 2023, CBP issued new guidance instructing its offices to review these claims. By enabling the claim targeting feature in ACE to randomly target claims for review, CBP should be better positioned to protect U.S. trade revenue from improper payment of drawback claims.[12]

- DHS addressed two recommendations related to countering violent extremism. First, DHS took steps to revise and augment its strategies related to counterterrorism and targeted violence.[13] In 2023, DHS completed a comprehensive assessment of all relevant strategies to consolidate and prioritize the department's critical counterterrorism action items. Through this assessment, DHS incorporated additional key elements of a comprehensive strategy that were not included in the 2019 Strategy, such as identifying needed resources and external factors that could affect goals. By taking these actions, DHS is better positioned to make informed decisions about its counterterrorism efforts, including setting priorities, allocating resources, and identifying program improvements when needed.

  Second, DHS took steps to incorporate targeted violence and terrorism prevention into its data governance framework.[14] For instance, the department identified the data domains that would govern targeted violence and terrorism prevention data. Further, as of January 2024, DHS published a department-wide learning agenda, which is a mechanism to capture DHS skills and capabilities required to meet mission goals, including those associated with targeted violence and terrorism prevention. By taking these actions, DHS is better positioned to leverage data to support and inform its targeted violence and terrorism prevention efforts, including building effective policy to address threats and trends it identifies in the data.

- In 2023, the Transportation Security Administration (TSA) took steps to improve its risk ranking tool used to assess pipeline systems.[15] As a result of addressing our two recommendations, TSA updated its risk ranking tool with improved data sources and continues to explore additional data for use in future years. TSA also completed a peer review of its pipeline risk ranking tool to help ensure that it is using a comprehensive and accurate methodology. TSA is now better positioned to identify pipeline relative risk and to more accurately target federal resources toward reducing vulnerabilities of high-risk pipeline networks.

- In March 2024, the Cybersecurity and Infrastructure Security Agency (CISA) developed methods for determining adoption of the National Institute of Standards and Technology's

---

[12]GAO, *Customs and Border Protection: Risk Management for Tariff Refunds Should Be Improved*, GAO-20-182 (Washington, D.C.: December 17, 2019).

[13]GAO, *Countering Violent Extremism: DHS Can Further Enhance Its Strategic Planning and Data Governance Efforts*, GAO-21-507 (Washington, D.C.: July 20, 2021).

[14]GAO-21-507.

[15]GAO, *Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management*, GAO-19-48 (Washington, D.C.: December 18, 2018).

cybersecurity framework among critical infrastructure sectors.[16] Specifically, CISA developed cross-sector cybersecurity performance goals that align with the cybersecurity framework and has begun measuring sectors' adoption of the cross-sector goals. By taking these steps, CISA has a more comprehensive understanding of how the framework's use is impacting critical infrastructure protection efforts.

- In August 2023, DHS took steps to track and monitor all Homeland Advanced Recognition Technology (HART) program costs.[17] Specifically, DHS officials included government labor costs in the program's 2022 life cycle cost estimate and demonstrated ongoing updates to the estimate. By taking these actions, the program and oversight bodies should be able to have an accurate account of program spending and compare actual costs against planned estimates.

- In December 2023, DHS took steps to fully define and document the role of privacy officials in reviewing and approving privacy protections for systems that contain personally identifiable information (PII).[18] Specifically, in its guidance for sensitive systems, DHS defined the roles and responsibilities of the senior agency official for privacy and other privacy officials for reviewing and approving system categorizations, overseeing privacy control assessments, and reviewing authorization packages. By taking these actions, DHS is better positioned to ensure that privacy protections are adequately incorporated into systems with PII.

We ask for your continued attention to the 26 remaining priority recommendations. We are also adding 11 new recommendations, bringing the total number of priority recommendations to 37. (See the Enclosure for the list of recommendations.)

First, in light of recent events, DHS should ensure that special agents assigned to the Presidential Protective Division (PPD) and the Vice Presidential Protective Division (VPD) of the Secret Service reach annual training targets given current and planned staffing levels. Developing and implementing a plan for meeting protection-related training targets would better prepare special agents to effectively respond to the security threats faced by the President and other protectees. The Secret Service must be prepared to face evolving threats in a rapidly changing environment. This involves having certain specific security skills and routine training on an ongoing basis.[19]

In addition, we are making 10 other new recommendations related to collaborative efforts to counter domestic terrorism, reviewing information systems and bulk data owned by the DHS Office of Intelligence and Analysis, addressing challenges in DHS's Biometric Identity System,

---

[16]GAO, *Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption*, GAO-18-211 (Washington, D.C.: February 15, 2018).

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

[18]GAO, *Privacy: Dedicated Leadership Can Improve Program and Address Challenges*, GAO-22-105065 (Washington, D.C.: September 22, 2022).

[19]GAO, *U.S. Secret Service: Further Actions Needed to Fully Address Protective Mission Panel Recommendations*, GAO-19-415 (Washington, D.C.: May 22, 2019).

improving the National Cybersecurity Strategy, modernizing DHS's financial management systems, and ensuring the designs of the Coast Guard's additional Offshore Patrol Cutters and lead Polar Security Cutter are stable and mature respectively.

These 10, along with the 26 previous priority recommendations, fall into the following seven areas:

**Emergency Preparedness and Response.** Disasters affect numerous American communities and cause billions of dollars of damage. FEMA plays a key role in preparing local communities for emergencies, rapidly responding during crises, and supporting recovery. FEMA should implement five priority recommendations in this area. For instance, we recommended that FEMA should identify ways to better manage fragmentation across federal disaster recovery programs. Doing so would help FEMA improve service delivery to disaster survivors and communities, and improve the effectiveness of recovery efforts.

We also recommended that FEMA take steps to identify and address barriers to, and disparate outcomes from, disaster programs. This would better position FEMA and other federal agencies to address potential social and institutional barriers in disaster assistance programs. Further, we recommended that FEMA implement a methodology to more comprehensively assess a jurisdiction's capability to respond to a disaster without federal assistance. By implementing this recommendation, FEMA could more effectively limit the federal government's fiscal exposure.

**Border Security.** DHS is responsible for securing the nation's borders, while also facilitating lawful trade, travel, and immigration. In this role, DHS is charged with, among other things, ensuring the detection and interdiction of persons unlawfully entering the U.S., and protecting U.S. trade revenue. DHS should fully implement five priority recommendations in this area. First, we recommended that DHS collaborate with the Department of Health and Human Services (HHS) to address information sharing gaps to ensure that HHS receives information needed to make decisions for unaccompanied children, including those apprehended with an adult. Doing so would also enable HHS to make more informed and timely decisions for unaccompanied children. We also recommended that DHS better articulate a commonly agreed to outcome for Department of Defense (DOD) support to DHS's southwest border security mission. This would help both agencies have a clearer understanding of how DHS will manage its border security mission with its own assets.

Further, we recommended that CBP assess the feasibility of flagging excessive export submissions across multiple drawback claims to prevent over claiming. Because claimants could over claim drawback refunds for merchandise that was never exported, having the ability to flag excessive export submissions across multiple claims would enhance CBP's protection against over claiming. We also recommended that CBP develop a plan, with time frames, to establish a reliable system of record for proof of export. Without an electronic means of establishing proof of export, the U.S. government may be subject to revenue loss through duplicate or excessive claims for drawback related to export information. Lastly, we recommended that DHS improve risk management in its collection and refund of duties. Improving risk management could help CBP strategically mitigate the effects of antidumping and countervailing duty nonpayment.

**Countering Violent Extremism and Domestic Terrorism.** Violent extremism—generally defined as planning or committing violent acts to achieve political, ideological, religious, or social

goals—has been perpetrated and promoted by a broad range of individuals and groups. Violent extremists continue to be a threat to the homeland. DHS tracked a total of 231 domestic terrorism incidents from 2010 to 2021, resulting in 145 deaths in the U.S. Further, according to our analysis of Federal Bureau of Investigation (FBI) data, the number of FBI's open domestic terrorism-related cases grew by 357 percent from 1,981 to 9,049 (from 2013 to 2021).

DHS should fully implement the two priority recommendations in this area. The first is to coordinate with the FBI to assess existing formal agreements for working together and sharing information to counter domestic terrorism. The second is to establish common terminology for the term "targeted violence." Taking these steps can better position DHS to identify and counter domestic threats.

**Domestic Intelligence and Information Sharing.** In the weeks preceding January 6, 2021, DHS was among several federal, state, and local entities responsible for identifying and sharing information or coordinating security measures to protect the U.S. Capitol. GAO identified six priority recommendations related to improving DHS's domestic intelligence capabilities and information sharing.

First, we recommended that DHS clarify policies regarding what factors merit National Special Security Event designation and who can request this designation. By doing so, DHS would be better positioned to ensure that its process to designate special security events is responsive to changing threats and understood by relevant agencies. Further, because DHS did not process or share all threat-related information with relevant agencies, we recommended that DHS assess internal controls related to these activities. Identifying and addressing internal control deficiencies can help ensure that DHS personnel consistently follow policies for developing and sharing threat products and can help provide information to increase DHS and its partners' awareness of potential threats. GAO also found that DHS did not conduct required reviews of information systems and bulk data.[20] Implementing the two priority recommendations related to these reviews would help ensure that appropriate measures were taken to protect the privacy, civil rights, and civil liberties of U.S. citizens.

**Information Technology and Cybersecurity.** DHS and its components invest billions of dollars each year to acquire IT and other capabilities to support the department's functions. Many of DHS's major IT acquisition programs have taken longer than expected to develop or have failed to deliver the desired value.

DHS should fully implement GAO's eight priority recommendations in this area. These recommendations include implementing leading practices for network capacity planning for the U.S. Coast Guard to better position the agency in mitigating risks resulting from inefficiencies and disruptions in network availability for its users. In addition, we recommended that DHS ensure the biometric identity management system modernization program (referred to as the Homeland Advanced Recognition Technology program) revises the schedule estimate to

[20]These reviews are required by the Intelligence Oversight Guidelines issued by the DHS Office of Intelligence and Analysis. The reviews of information systems are to assess whether DHS personnel had appropriate clearances to access information about U.S. persons, among other safeguards. The reviews of bulk data are to assess whether DHS personnel's access to, and searches conducted in, bulk data were appropriately limited to protect the privacy, civil rights, and civil liberties of U.S. persons.

incorporate scheduling best practices to limit further schedule delays and cost overruns in modernizing its 29-year-old legacy system. Further, we recommended that DHS comprehensively assess the methods used to share cyber threat information with critical infrastructure entities to ensure that the sharing methods used by the agencies is the optimal approach to addressing cyber threat sharing challenges. Implementing the priority recommendations, such as these, would help improve key DHS programs and help the agency improve service delivery.

DHS has also faced significant internal control deficiencies that have contributed to GAO designating DHS financial management as high risk. We have monitored DHS's financial management challenges as part of our High-Risk List since 2003.[21] To address its financial management issues, DHS is executing a multiyear plan, that includes modernizing its financial management systems at Coast Guard, FEMA, and U.S. Immigration and Customs Enforcement (ICE). DHS intends for these modernized systems to help it comply substantially with the Federal Financial Management Improvement Act of 1996.[22] DHS should fully implement the priority recommendations in this area, including the Joint Program Management Office work with Coast Guard, FEMA, and ICE to remediate issues identified by system testing.

**Chemical Security.** Thousands of high-risk chemical facilities, comprising key U.S. critical infrastructure, may be subject to the risk posed by cyber threat adversaries—terrorists, criminals, or nations. These adversaries could potentially manipulate facilities' information and control systems to release or steal hazardous chemicals and inflict mass causalities to surrounding populations. CISA evaluates high-risk chemical facilities' cybersecurity efforts via inspections that include reviewing policies and procedures, interviewing relevant officials, and verifying facilities' implementation of agreed-upon security measures.

By implementing one priority recommendation in this area—developing a workforce plan that addresses cybersecurity-related needs—CISA could ensure that it has the appropriate number and type of staff to carry out its chemical program's cybersecurity efforts.[23] **Infrastructure, Acquisition, and Management.** DHS is the third-largest cabinet-level department in the federal government, overseeing tens of billions of dollars in annual budgetary resources, and employing more than 240,000 staff in a broad range of jobs. These jobs include countering terrorism and

[21]See GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, GAO-23-106203 (Washington, D.C.: April 20, 2023). In 2003, we designated *Implementing and Transforming DHS* as a high-risk area. In 2013, noting DHS's considerable progress, we narrowed the scope of the high-risk area to *Strengthening DHS Management Functions*. In 2023, we further narrowed the scope to *Strengthening DHS IT and Financial Management Functions* to focus on areas that continue to experience significant challenges.

[22]The Federal Financial Management Improvement Act requires 24 federal executive agencies, including DHS, to implement and maintain financial management systems that comply substantially with (1) federal financial management system requirements, (2) applicable federal accounting standards, and (3) the *U.S. Standard General Ledger* at the transaction level. Pub. L. No. 104-208, div. A, § 101(f), title VIII, 110 Stat. 3009, 3009-389 (1996), *reprinted in* 31 U.S.C. § 3512 note.

[23]As of July 28, 2023, the statutory authority for DHS's chemical security program has expired. Therefore, further updates are pending reauthorization.

homeland security threats, and providing aviation and border security, emergency response, cybersecurity, and critical infrastructure protection.

DHS should fully implement nine priority recommendations in this area. Some of these include DHS employing models for the U.S. Coast Guard's asset lines for predicting the outcome of investments, analyzing trade-offs, and optimizing decisions among competing investments. This will better position the Coast Guard to identify and achieve potential cost savings.

Further, DHS should ensure that the Coast Guard's Offshore Patrol Cutter stage 2 program achieves 100 percent completion of basic and functional design, including routing of major distributive systems and transitive components that effect multiple zones of the ship, prior to the start of lead ship construction. This will reduce the risk of costly rework and further delays in delivering capability. Finally, DHS should ensure the functional design for the lead Polar Security Cutter is complete, including routing of major distributive systems that affect multiple zones of the ship, prior to authorizing lead cutter construction beyond the previously approved eight prototype units. This will ensure the design is mature, limiting the risk of further delays and costly rework.

Also, DHS should start using a balanced set of performance metrics to manage the department's procurement organizations. This will help DHS better identify improvement opportunities, set priorities, and allocate resources. In implementing these recommendations, DHS could ensure its infrastructure, assets, workforce, and procurement organizations are effectively managed to accomplish DHS's wide range of missions. In addition, if implemented, taking some of these actions could potentially lead to millions or a hundred million or more annually in potential savings.

As the auditor of the consolidated financial statements of the U.S. government, and as noted above, I have observed that the Department of Homeland Security received an adverse opinion on its internal control over financial reporting for fiscal year 2023, due to five material weaknesses in its internal control over financial reporting, including weaknesses related to information system controls and insurance liabilities. These weaknesses, as well as related auditor recommendations, are important issues. I encourage you to devote significant attention to address them and achieve a clean opinion on internal control over financial reporting, which would provide the department with reliable financial information for effective management and decision-making.

Also, in April 2023, we issued our biennial update to our High-Risk List. This list identifies government operations with greater vulnerabilities to fraud, waste, abuse, and mismanagement. It also identifies the need for transformation to address economy, efficiency, or effectiveness challenges.[24] One of our high-risk areas, Strengthening Department of Homeland Security IT and Financial Management Functions, centers directly on DHS. Another high-risk area is related to FEMA's management of the National Flood Insurance Program.

Several other government-wide high-risk areas also have direct implications for DHS and its operations. These include (1) improving the management of IT acquisitions and operations, (2)

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

improving strategic human capital management, (3) managing federal real property, and (4) managing the government-wide personnel security clearance process.

Another high-risk area where DHS has a critical role is ensuring the cybersecurity of the nation. Integral to fulfilling that mission is the department's CISA. In October 2022, we recommended that CISA develop metrics for measuring the effectiveness of its K-12 cybersecurity-related products and services that are available for school districts.[25] Additionally, in February 2023, we recommended that CISA establish milestones and timelines for its efforts to provide guidance and improve coordination and information sharing to help critical infrastructure Sector Risk Management Agencies.[26] Further, in January 2024, we made a number of recommendations that DHS and CISA work to better understand and measure the effectiveness of selected critical infrastructure sectors' cybersecurity practices that reduce the risk of ransomware.[27]

In addition to DHS's high-risk areas, we urge your continued attention to the government-wide high-risk issues as they relate to DHS. Progress on high-risk issues has been possible through the concerted actions and efforts of Congress, the Office of Management and Budget (OMB), and the leadership and staff in agencies, including within DHS. In March 2022, we issued a report on key practices to successfully address high-risk areas, which can be a helpful resource as your agency continues to make progress to address high-risk issues.[28]

We also recognize the key role Congress plays in providing oversight and maintaining focus on our recommendations to ensure they are implemented and produce their desired results. Legislation enacted in December 2022 includes a provision for GAO to identify any additional congressional oversight actions that can help agencies implement priority recommendations and address any underlying issues relating to such implementation.[29]

Congress can use various strategies to address our recommendations, such as incorporating them into legislation. Congress can also use its budget, appropriations, and oversight processes to incentivize executive branch agencies to act on our recommendations and monitor their progress. For example, Congress can hold hearings focused on DHS's progress in implementing GAO's priority recommendations, withhold funds when appropriate, or take other actions to provide incentives for agencies to act. Moreover, Congress could follow up during the appropriations process and request periodic updates.

---

[25]GAO, *Critical Infrastructure Protection: Additional Federal Coordination Is Needed to Enhance K-12 Cybersecurity*, GAO-23-105480 (Washington, D.C.: Oct. 20, 2022).

[26]GAO, *Critical Infrastructure Protection: Time Frames to Complete DHS Efforts Would Help Sector Risk Management Agencies Implement Statutory Responsibilities*, GAO-23-105806 (Washington, D.C.: Feb. 7, 2023).

[27]GAO, *Critical Infrastructure Protection: Agencies Need to Enhance Oversight of Ransomware Practices and Assess Federal Support*, GAO-24-106221 (Washington, D.C.: Jan. 30, 2024).

[28]GAO, *High-Risk Series: Key Practices to Successfully Address High-Risk Areas and Remove Them from the List*, GAO-22-105184 (Washington, D.C.: Mar. 3, 2022).

[29]James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263, § 7211(a)(2), 136 Stat. 2395, 3668 (2022); H.R. Rep. No. 117-389 (2022) (accompanying Legislative Branch Appropriations Act, H.R. 8237, 117th Cong. (2022)).

Congress also plays a key role in addressing any underlying issues related to the implementation of these recommendations. For example, Congress could pass legislation providing an agency explicit authority to implement a recommendation or requiring an agency to take certain actions to implement a recommendation.

Copies of this report are being sent to the Director of OMB and the appropriate congressional committees. In addition, the report will be available on the GAO website at Priority Open Recommendation Letters | U.S. GAO.

I appreciate DHS's continued commitment to these important issues. If you have any questions or would like to discuss any of the issues outlined in this letter, please do not hesitate to contact me or Jason L. Bair, Managing Director, Homeland Security and Justice Team at BairJ@gao.gov or (202) 512-6881. Contact points for our offices of Congressional Relations and Public Affairs may be found on the last page of this report. Our teams will continue to coordinate with your staff on all the 478 open recommendations, as well as those additional recommendations in the high-risk areas for which DHS has a leading role. Thank you for your attention to these matters.

Sincerely,

Gene L. Dodaro
Comptroller General
of the United States

Enclosure

cc: Kristie Canegallo, Senior Official Performing the Duties of the Deputy Secretary

Randolph D. “Tex” Alles, Deputy Under Secretary for Management
The Honorable Deanne Criswell, Administrator, Federal Emergency Management Agency (FEMA)

Nick Shufro, Deputy Assistant Administrator, Risk Management Directorate, Federal Insurance and Mitigation Administration, Resilience, FEMA
Troy Miller, Senior Official Performing the Duties of the Commissioner, U.S. Customs and Border Protection
The Honorable Ur Mendoza Jaddou, Director, U.S. Citizenship and Immigration Services
Jason Owens, Chief, United States Border Patrol
The Honorable David P. Pekoske, Administrator, Transportation Security Administration

Admiral Linda L. Fagan, Commandant of the Coast Guard, U.S. Coast Guard

The Honorable Kenneth L. Wainstein, Under Secretary, Office of Intelligence and Analysis

Roland Edwards, Chief Human Capital Officer, Office of the Chief Human Capital Officer
The Honorable Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency (CISA)
Bill Pratt, Director, Strategic Technology Management, Chief Technology Officer Directorate, Office of the Chief Information Officer

Michael Weissman, Chief Data Officer

Shonnie Lyon, Director, Office of Biometric Identity Management

Paul Courtney, Chief Procurement Officer
James Murray, Acting Director, Financial Systems Modernization Joint Program Management Office

The Honorable Mary Ellen Callahan, Assistant Secretary, Countering Weapons of Mass Destruction Office
Dr. David Mussington, Executive Assistant Director for Infrastructure Security, CISA

The Honorable Robert Silvers, Under Secretary, Office of Strategy, Policy, and Plans

Jeohn Favors, Assistant Secretary for Counterterrorism, Threat Prevention and Law Enforcement

Ronald L. Rowe, Jr., Acting Director, U.S. Secret Service

The Honorable Shalanda Young, Director, Office of Management and Budget

**Enclosure**

**Priority Open Recommendations to the Department of Homeland Security**

*U.S. Secret Service: Further Actions Needed to Fully Address Protective Mission Panel Recommendations*. GAO-19-415. Washington, D.C.: May 22, 2019.

**Year Recommendation Made:** 2019

**Recommendation:** The Director of the Secret Service should develop and implement a plan to ensure that special agents assigned to Presidential Protective Division and Vice Presidential Protective Division reach annual training targets given current and planned staffing levels.

**Action Needed:** DHS concurred with our recommendation.

On September 19, 2014, an intruder jumped over the north fence of the White House complex, passed several layers of security, evaded Secret Service personnel, and entered the White House through the north portico doors. The President was not in the White House at the time. In October 2014, the Secretary of Homeland Security established the U.S. Secret Service Protective Mission Panel (Panel). The Panel's final report, issued December 2014, concluded that the September 2014 incident occurred in large part because of a "catastrophic failure in training.[30] The Panel's first recommendation was for the Secret Service to provide a true "Fourth Shift" for training the Presidential Protective Division (PPD) and Vice-Presidential Protective Division (VPD), so that they spend 2 weeks out of every 8 in training (i.e., 25 percent of work time), and ensure that Uniformed Division officers are in training for no less than 10 percent of their time.

In May 2019, we reported that the Secret Service had not met the established training target (25 percent of work time) and lacked a plan for achieving it. Specifically, we found that, in fiscal year 2018, PPD and VPD special agents reported attending training for 5.9 percent and 2.9 percent of their regular work hours, respectively. We therefore recommended that the Director of the Secret Service develop and implement a plan to ensure that special agents assigned to the PPD and VPD reach annual training targets given current and planned staffing levels. The agency concurred with our recommendation but told us that the agency no longer agreed with the 25 percent training target and planned to reevaluate it as of May 2019. Secret Service has taken the following steps since then.

- In August 2021, the Secret Service issued its Human Capital Strategic Plan for Fiscal Years 2021-2025, including information on staffing needed to meet stated training requirements. This plan set new annual training targets for special agents assigned to PPD and VPD to be approximately 12 percent. However, in September 2021, Secret Service officials told us that they did not anticipate being able to meet the new training target until they reach planned staffing level targets in fiscal year 2025.

- In May 2022, Secret Service provided us with training data regarding time PPD and VPD special agents spent in training. Based on our analysis, PPD and VPD spent an average of 8.7 and 6.6 percent of their regular work hours in training since August 2021. Although these percentages are higher than at the time of our report, Secret

[30]See U.S. Secret Service Protective Mission Panel, *Report from the United States Secret Service Protective Mission Panel to the Secretary of Homeland Security* (Washington, D.C.: Dec. 15, 2014).

Service had not yet reached or developed a plan to reach the near-term 12 percent training target, given its current staffing levels.

- In March 2023, Secret Service provided us with a training plan for PPD and VPD to reach its 12 percent revised training goal. The plan states that Secret Service will work with DHS, OMB, and Congress to secure funding for additional personnel so that the agency could increase the available time to train for PPD and VPD agents. The plan details that, if the funding were to be secured, PPD and VPD agents could gradually start increasing the time spent in training, reaching the agency's 12 percent goal in 2027. This plan is based on a number of other assumptions that Secret Service specified, including additional funding from Congress for Secret Service's training facilities, and similar protectee counts. This plan shifted Secret Service's target timeframe for meeting its revised 12 percent goal another two years into the future to 2027, compared to September 2021 when the Secret Service estimated that it would reach its target goal in 2025.

- As of August 2023, no further action had been taken. Affected special agents may continue to lack training required to prevent security breaches, such as that of September 19, 2014, when an intruder jumped the north fence and entered the White House. Trained special agents are critical to ensuring the safety and security of presidents and other protectees, as underscored by the July 2024 assassination attempt of former President Trump.

- In July 2024, we requested an update on the status of this recommendation. As of August 2024, Secret Service had not yet provided additional information.

To fully implement this recommendation, the Secret Service needs to develop and implement a plan to ensure that special agents assigned to PPD and the VPD reach annual training targets given current and planned staffing levels.

**Director:** Triana McNeil, Homeland Security and Justice

**Contact information:** McNeilT@gao.gov, (202) 512-8777

**Emergency Preparedness and Response**

*Federal Disaster Assistance: Improved Criteria Needed to Assess a Jurisdiction's Capability to Respond and Recover on Its Own*. GAO-12-838. Washington, D.C.: September 12, 2012**.**

**Year Recommendation Made:** 2012

**Recommendation:** To increase the efficiency and effectiveness of the process for disaster declarations, the FEMA Administrator should develop and implement a methodology that provides a more comprehensive assessment of a jurisdiction's capability to respond to and recover from a disaster without federal assistance. This should include one or more measures of a jurisdiction's fiscal capacity, such as Total Taxable Resources, and consideration of the jurisdiction's response and recovery capabilities. If FEMA continues to use the Public Assistance per capita indicator to assist in identifying a jurisdiction's capabilities to respond to and recover from a disaster, it should adjust the indicator to accurately reflect the annual changes in the U.S. economy since 1986, when the current indicator was first adopted for use. In addition, implementing the adjustment by raising the indicator in steps over several years would give jurisdictions more time to plan for and adjust to the change.

**Action Needed:** FEMA concurred with this recommendation. FEMA has taken steps to update the factors considered when evaluating a request for a major disaster declaration for Public Assistance. Specifically, FEMA proposed updating the estimated cost of assistance (i.e., the per capita indicator) three times (in 2016, 2017, and 2020), via the federal rulemaking process.

However, as of February 2024, the agency has not issued a final rule updating the estimated cost of assistance nor does it intend to take additional actions to implement our recommendation. Until FEMA fully implements a new methodology, the agency will not have an accurate assessment of a jurisdiction's capabilities to respond to and recover from a disaster without federal assistance. Until such time, FEMA continues to run the risk of recommending the President award Public Assistance to jurisdictions that have the capability to respond and recover on their own.

**High Risk Area:** Limiting the Federal Government's Fiscal Exposure by Better Managing Climate Change Risks

**Director:** Christopher P. Currie, Homeland Security and Justice
**Contact information:** CurrieC@gao.gov, (202) 512-8777

*Disaster Recovery: Actions Needed to Improve the Federal Approach*. GAO-23-104956. Washington, D.C.: November 15, 2022.

**Year Recommendations Made:** 2023

**Recommendation:** The FEMA Administrator should, in consultation with the Recovery Support Function Leadership Group, identify and take steps to better manage fragmentation between its disaster recovery programs and other federal programs, including consideration of the options identified in the report. If FEMA determines that it needs authority for actions that it seeks to implement, it should request that authority from Congress.

**Action Needed:** DHS agreed with this recommendation. As of February 2024, FEMA officials stated that they were continuing to work with the White House and senior executives across the federal government through the Recovery Support Function Leadership Group (RSFLG) and Interagency Policy Committee to consider options to improve disaster recovery, including those identified by GAO. FEMA has also worked with the Small Business Administration (SBA), U.S. Department of Housing and Urban Development (HUD), OMB and other interagency partners to explore the viability of a single disaster assistance application, aligned with one of the options identified by GAO.

Further, FEMA officials told us they were collaborating with HUD to determine a path forward for HUD to be the inaugural partner in a consolidated application for individual disaster assistance. FEMA officials stated that they were not able to identify an approach for a consolidated application with SBA, but they are working together toward improved data sharing of common applicant data elements and a "no wrong door" approach. According to FEMA officials, this approach would ensure that disaster survivors who could benefit from working with both agencies are fully aware of the types of assistance available to them and are appropriately guided directly into each Agency's registration intake process with their common data.

FEMA's work through the Interagency Policy Committee, RSFLG, and directly with HUD and SBA on the possibility of a common application could help FEMA identify and take steps to better manage fragmentation between FEMA's disaster recovery programs and other federal programs, including consideration of the options in our report. To fully address this

recommendation, FEMA will need to demonstrate that it has worked with interagency partners and thoroughly considered available options, identified those it intends to implement, and then take steps to do so. By taking these steps, FEMA could improve service delivery to disaster survivors and communities and improve the effectiveness of recovery efforts.

**Recommendation:** The FEMA Administrator should identify and take steps to better manage fragmentation across its disaster recovery programs, including consideration of the options identified in this report. If FEMA determines that it needs authority for actions that it seeks to implement, it should request that authority from Congress.

**Action Needed:** DHS agreed with this recommendation. In response, FEMA has taken steps to streamline applications for its Individual Assistance and Public Assistance programs to reduce the complexity and time it takes to apply. According to FEMA documentation, as of February 2024, FEMA has begun implementing some of these changes, such as streamlining the online disaster survivor registration intake process in fall 2023. FEMA officials explained that they were also in the process of revising their Public Assistance intake forms to eliminate duplicate requests for information by pre-populating answers the applicant already provided. FEMA officials estimate that the changes to these forms will reduce the administrative burden by around 20 percent. FEMA officials stated that other changes, such as removing the requirement that survivors apply for an SBA loan before being considered for certain types of financial assistance, went into effect for disasters declared after March 22,2024.

To fully address this recommendation FEMA will need to demonstrate that it has thoroughly considered available options to reduce fragmentation across its own programs, identified those it intends to implement, and then taken steps to do so. By taking these steps, FEMA could make its programs simpler, more accessible, and more user-friendly, thereby improving their effectiveness.

**Director:** Christopher P. Currie, Homeland Security and Justice
**Contact information:** CurrieC@gao.gov, (202) 512-8777

*Disaster Recovery: Additional Actions Needed to Identify and Address Potential Recovery Barriers*. GAO-22-104039. Washington, D.C.: December 15, 2021.

**Year Recommendations Made:** 2022

**Recommendation:** The FEMA Administrator should, in coordination with the SBA Associate Administrator of the Office of Disaster Assistance and the HUD Assistant Secretary for Community Planning and Development, develop, with input from key recovery partners, and implement an interagency plan to help ensure the availability and use of quality information that includes (1) information requirements, (2) data sources and methods, and (3) strategies for overcoming information challenges—to support federal agencies involved in disaster recovery in identifying access barriers or disparate outcomes.

**Action Needed:** DHS agreed with this recommendation. In June 2024, FEMA officials told us that FEMA, together with HUD and SBA, are developing an interagency plan for data collection, sharing, and analysis to identify potential equity issues. According to FEMA, this interagency plan will be developed by August 2024. They also noted that in November 2023, FEMA completed Privacy Threshold Analyses needed to share certain aggregate applicant data with HUD and SBA to help all three agencies identify potential access barriers.

To fully address the recommendation and ensure the availability and use of quality information needed to identify access barriers and disparate outcomes, FEMA (with HUD and SBA) will need to both develop and implement this interagency plan specifying the data needed, the sources of those data, and the methods for obtaining those data. Without implementing a plan to ensure the availability of comprehensive information, disaster recovery programs lack a means to identify potential social and institutional barriers in their own programs and across programs.

**Recommendation:** The FEMA Administrator should coordinate with the SBA Associate Administrator of the Office of Disaster Assistance and the HUD Assistant Secretary for Community Planning and Development to design and establish routine processes to be used within and across federal disaster recovery programs to address identified access barriers and disparate outcomes on an ongoing basis.

**Action Needed:** DHS agreed with this recommendation. In June 2024, FEMA officials told us that, together with HUD and SBA, they are developing an interagency plan that includes a description of routine processes that will be used to address any equity issues they identify. According to FEMA, this interagency plan will be developed by August 2024. FEMA officials stated that they anticipate addressing the identified access barriers through targeted capacity-building support, including: training, peer-to-peer network development, recovery planning, and technical assistance to help local and tribal governments with high vulnerability indicators to better manage recovery efforts.

To fully address the recommendation, FEMA (with HUD and SBA) must also implement institutionalized processes to be used within and across federal recovery programs to address identified access barriers and disparate outcomes on an ongoing basis. Without routine processes, disaster recovery programs lack a mechanism to ensure they can address any potential access barriers or disparate outcomes they might identify, particularly if the cause of those barriers or outcomes arise from the interaction between or among programs.

**Director:** Christopher P. Currie, Homeland Security and Justice
**Contact information:** CurrieC@gao.gov, (202) 512-8777

**Border Security**

*Antidumping and Countervailing Duties: CBP Action Needed to Reduce Duty Processing Errors and Mitigate Nonpayment Risk.* GAO-16-542. Washington, D.C.: July 14, 2016.

**Year Recommendation Made:** 2016

**Recommendation:** To improve risk management in the collection of Antidumping and Countervailing (AD/CV) duties, CBP should, consistent with U.S. law and international obligations, take steps to use its data and risk assessment strategically to mitigate AD/CV duty nonpayment, such as by using predictive risk analysis to identify entries that pose heightened risk and taking appropriate action to mitigate the risk.

**Action Needed:** DHS concurred with this recommendation. As of February 2024, CBP had issued guidance for determining when to use a single transaction bond (STB) for AD/CV entries and updated its monetary guidelines for setting bond amounts. CBP had also issued guidance to revoke CBP officials' authority to allow importers that it suspended or debarred to use a continuous entry bond, except when this bond is the only type acceptable.

CBP officials said they are in the process of (1) updating their electronic bond regulation to formally allow the use of an electronic bond and (2) automating their bond sufficiency checks. According to CBP officials, the agency plans to complete these two initiatives by the end of September 2024. The initiatives CBP has taken and plans to take could help CBP mitigate the risk of AD/CV duty nonpayment but none use CBP's data and risk analysis strategically as GAO's recommendation intended.

**Managing Director:** Kimberly M. Gianopoulos, International Affairs and Trade
**Contact information:** GianopoulosK@gao.gov, (202) 512-8612

*Southwest Border: Actions Needed to Improve DHS Processing of Families and Coordination between DHS and HHS*. GAO-20-245. Washington, D.C.: February 19, 2020.

**Year Recommendation Made:** 2020

**Recommendation:** The Secretary of Homeland Security, jointly with the Secretary of HHS, should collaborate to address information sharing gaps identified in this report to ensure that the Office of Refugee Resettlement (ORR) receives information needed to make decisions for unaccompanied alien children (UAC), including those apprehended with an adult.

**Action Needed:** DHS concurred with this recommendation. In coordination with HHS, DHS implemented the Unified Immigration Portal, which provides real time data to help track unaccompanied children from the time of DHS apprehension to their referral and placement in HHS-funded facilities, including those who are apprehended with an adult. Additionally, HHS continues to implement its case management data system, which is integrated with the Unified Immigration Portal. This helps HHS officials retrieve information about a child's case more quickly and automates the process for referring unaccompanied children from DHS to HHS.

However, as of March 2024, the information gaps we highlighted in our report continue to exist. In particular, ORR officials stated they do not consistently receive information from DHS about the adults who arrived with unaccompanied children. This would help ORR make placement and release decisions. In the fall of 2023, DHS reported it was working with ORR on a new interagency agreement to govern information sharing. DHS stated it anticipates concluding work on the new agreement by August 2024.

To fully address the recommendation, DHS and HHS should finalize their information sharing agreement and ensure the agreement addresses information sharing gaps identified in our report. Doing so would help ensure that ORR receives information needed to make decisions for unaccompanied children, including those apprehended with an adult. Doing so would also enable ORR to make more informed and timely decisions for unaccompanied children, including those separated from adults with whom they were apprehended.

**Director:** Rebecca S. Gambler, Homeland Security and Justice
**Contact information:** GamblerR@gao.gov, (202) 512-8777

*Customs and Border Protection: Risk Management for Tariff Refunds Should Be Improved*. GAO-20-182. Washington, D.C.: December 17, 2019.

**Year Recommendations Made:** 2020

**Recommendation:** The Commissioner of CBP should ensure that the Office of Trade assesses the feasibility of flagging excessive export submissions across multiple claims and takes cost-effective steps, based on the assessment, to prevent over claiming.

**Action Needed:** CBP concurred with this recommendation. In March 2023, CBP drafted a white paper examining the feasibility of attaching a unique identifier to exported merchandise in the Automated Commercial Environment (ACE) and mandating a uniform reporting requirement of the exported merchandise's unique identifier. Based on the assessment, CBP determined that tracking export submissions across drawback claims is not feasible because current law, ACE programming, and staff resources do not support the uniform reporting requirement CBP was considering.[31]

In February 2024, CBP officials told us that tracking export submissions across drawback claims would require a long-term plan to develop ACE capabilities, set priorities, and align resources. To fully implement the recommendation, CBP needs to finalize its plan. Because claimants could over claim drawback refunds for merchandise that was never exported, having the ability to flag excessive export submissions across multiple claims would enhance CBP's protection against over claiming.

**Recommendation:** The Commissioner of CBP should ensure that the Office of Trade develops a plan, with time frames, to establish a reliable system of record for proof of export.

**Action Needed:** CBP concurred with this recommendation. In November 2023, CBP drafted a white paper examining the suitability of the Automated Export System (AES) as an electronic means of establishing proof of export. Based on the assessment, CBP determined that AES cannot support electronic proof of export for drawback claims in its current state.

In February 2024, CBP officials told us that establishing a reliable system of record for proof of export would require a long-term plan to develop AES capabilities, set priorities, and align resources. To fully implement the recommendation, CBP needs to finalize its plan. Until CBP implements effective control activities for the drawback program, the U.S. government may be subject to revenue loss through duplicate or excessive claims for drawback related to export information.

**Managing Director:** Kimberly M. Gianopoulos, International Affairs and Trade
**Contact information:** GianopoulosK@gao.gov, (202) 512-8612

*Southwest Border Security: Actions Are Needed to Address the Cost and Readiness Implications of Continued DOD Support to U.S. Customs and Border Protection*. GAO-21-356. Washington, D.C.: February 23, 2021.

**Year Recommendation Made:** 2021

**Recommendation:** The Secretary of Homeland Security, together with the Secretary of Defense, should define a common outcome for DOD support to DHS, consistent with best practices for interagency collaboration, and articulate how that support will enable DHS to achieve its southwest border security mission in fiscal year 2021 and beyond.

**Action Needed:** DHS concurred with this recommendation. DHS stated that it will continue to use the request for assistance process to define and articulate a common outcome for DOD's

[31]Through the drawback program, CBP refunds up to 99 percent of duties, taxes, or fees previously paid by an importer. CBP makes these refunds on imported goods on which the importer previously paid duties, taxes, or fees, and subsequently exported from the U.S. or destroyed.

support to DHS. However, as we stated in our report, this process has not enabled DOD and DHS to agree to a common outcome for DOD's support, because it focuses on meeting DHS's operational requirements over a short period of time. DHS has continued to submit requests for assistance to DOD through fiscal year 2025.

As of March 2024, DHS has taken steps toward implementing our recommendation. Specifically, DHS officials told us that the Secretary of Homeland Security and the Secretary of Defense mutually desire an end to regular, yearly commitments of DOD capabilities in support of Customs and Border Protection's southwest border security mission. Customs and Border Protection has received some additional resources from Congress to apply to this mission according to those officials, which the agency has coupled with internal planning to provide a path to ending yearly DOD support.

We reviewed the DHS fiscal year 2024 and fiscal year 2025 requests for assistance and found that the "end of mission" section did not clearly state how both agencies will know when the mission has been completed. To fully implement the recommendation, DOD and DHS need to document the end of mission with an articulated common outcome. Doing so will help both agencies have a clearer understanding of how DHS will manage its border security mission with its own assets.

**Director:** Alissa Czyz, Director, Defense Capabilities and Management

**Contact information:** CzyzA@gao.gov, (202) 512-3058

**Countering Violent Extremism and Domestic Terrorism**

*Countering Violent Extremism: DHS Can Further Enhance Its Strategic Planning and Data Governance Efforts*. GAO-21-507. Washington, D.C.: July 20, 2021.

**Year Recommendation Made:** 2021

**Recommendation:** The Secretary of Homeland Security—in consultation with affected offices and components—should establish common terminology for targeted violence.

**Action Needed:** DHS concurred with this recommendation. DHS originally stated that it planned to add targeted violence to its approved DHS Lexicon by August 31, 2022. However, in May 2023, officials stated that the department was undergoing a reorganization that has affected the timeline for implementing this recommendation. As of March 2024, DHS developed a draft definition of targeted violence. To fully implement this recommendation, DHS will need to finalize the definition and add it to the approved DHS Lexicon. Without a common definition for targeted violence, it will be difficult for DHS to assess threats, track trends, and build effective policy within DHS and the stakeholder community.

**Director:** Triana McNeil, Homeland Security and Justice
**Contact information:** McNeilT@gao.gov, (202) 512-8777

*Domestic Terrorism: Further Actions Needed to Strengthen FBI and DHS Collaboration to Counter Threats*. GAO-23-104720. Washington, D.C.: February 22, 2023.

**Year Recommendation Made:** 2023

**Recommendation:** The DHS Under Secretary for Intelligence and Analysis should, in collaboration with the Director of the FBI, assess existing formal agreements to determine if they fully articulate a joint process for working together to counter domestic terrorism threats and sharing relevant domestic terrorism-related information and update and revise accordingly.

**Action Needed:** DHS concurred with this recommendation. As of March 2024, DHS has reviewed its formal agreements with the FBI. To fully implement this recommendation, DHS will need to coordinate with FBI to make any needed updates or revisions to existing agreements.

**Director:** Triana McNeil, Homeland Security and Justice

**Contact information:** McNeilT@gao.gov, (202) 512-8777

**Domestic Intelligence and Information Sharing**

*Capitol Attack: Special Event Designations Could Have Been Requested for January 6, 2021, but Not All DHS Guidance is Clear.* GAO-21-105255. Washington, D.C.: August 9, 2021.

**Year Recommendations Made:** 2021

**Recommendation:** The Secretary of Homeland Security should consider whether additional factors, such as the context of the events and surrounding circumstances in light of the current environment of emerging threats, are needed for designating NSSE events.

**Action Needed:** DHS officials stated that they did not concur with this recommendation. As of March 11, 2024, DHS believes that the process already is dynamic and responsive to change and requested that GAO consider the recommendation resolved and closed. We disagree and maintain that implementing this recommendation is important since the NSSE designation provides additional security measures such as placing the Secret Service as the operational lead for security for the event. We acknowledge that past congressional certifications of election results were not designated NSSEs, and DHS officials considered this normal congressional business. However, the lack of consideration of other factors, such as the large rally at the Ellipse that mobilized to the Capitol and the climate surrounding the 2020 election demonstrated a gap in how adaptable the event designation process is to such factors.

To fully implement this recommendation, DHS needs to formally review the factors it developed to designate an NSSE, including whether additional events should be designated as an NSSE. A review of these factors can help ensure that the process for designating an NSSE is dynamic and responsive to changing environments and emerging threats.

**Recommendation:** The Secretary of Homeland Security should update the Department of Homeland Security's policy to clarify and communicate the process for requesting an NSSE designation for an event held on federal property in Washington, D.C., to all relevant stakeholders, including relevant federal, state, and local entities.

**Action Needed:** DHS officials stated that they did not concur with this recommendation. As of March 11, 2024, DHS believes the process is understood by relevant stakeholders and requested that GAO consider the recommendation resolved and closed. We disagree and maintain that implementing this recommendation is important. As noted in our report, there is a gap in DHS's policy and in the awareness of relevant partners regarding the process. Clarifying and communicating the DHS policy for requesting an NSSE designation for events on federal

property in Washington, D.C. will help ensure that responsible entities are aware of their ability to make such a request.

To fully implement this recommendation, DHS needs to clarify its policy to identify who can request an NSSE designation on federal property in Washington, D.C. and communicate any updates to relevant stakeholders. Updating its policy will help DHS ensure that relevant agencies are aware of, and understand, the process for requesting such event designations and may help to better secure the Capitol Complex and other federal properties in the future.

**Director:** Triana McNeil, Homeland Security and Justice

**Contact information:** McNeilT@gao.gov, (202) 512-8777

*Capitol Attack: Federal Agencies Identified Some Threats, but Did Not Fully Process and Share Information Prior to January 6, 2021*. GAO-23-106625. Washington, D.C.: February 28, 2023

**Year Recommendations Made:** 2023

**Recommendation:** The DHS Under Secretary for Intelligence and Analysis (I&A) should assess the extent to which its internal controls ensure personnel follow existing and updated policies for processing open source threat information.

**Action Needed:** DHS concurred with this recommendation. DHS I&A established an internal controls branch, which, in fiscal year 2022, began the process of gathering foundational data to establish a systemic assessment process. As of May 22, 2024, DHS I&A officials told us they completed their initial 90-day review of I&A's open source intelligence program. DHS I&A is currently conducting an in-depth assessment of the design and effectiveness of the Open Source and Information Sharing processes and its newly implemented mitigating controls. According to I&A, during this assessment, they will perform walkthroughs and interviews with I&A stakeholders to discuss system implementation, processes, procedures and policies, and review corroborating evidence. Following the completion of the assessment, DHS I&A plans to provide the testing results, findings, and recommendations to I&A senior leadership. DHS I&A plans to complete these efforts by December 31, 2024.

However, gathering data is only the first step, and to fully implement this recommendation, DHS needs to complete the in-depth assessment of the Open Source and Information Sharing processes. Completing the assessment will provide DHS I&A with information to address internal control deficiencies and help ensure that personnel consistently follow existing and updated policies for processing open source threat information.

**Recommendation:** The DHS I&A Under Secretary should assess the extent to which its internal controls ensure personnel consistently follow the policies for sharing threat-related information with relevant agencies such as Capitol Police.

**Action Needed:** DHS concurred with this recommendation. DHS I&A established an internal controls branch, which, in fiscal year 2022, began the process of gathering foundational data to establish a systemic assessment process. As of May 22, 2024, DHS I&A officials told us they completed their initial 90-day review of I&A's open source intelligence program. DHS I&A is currently conducting an in-depth assessment of the design and effectiveness of the Open Source and Information Sharing processes to test its mitigating controls. DHS I&A plans to provide the results, findings, and recommendations to DHS I&A senior leadership, and once

finalized will provide the findings to GAO. DHS I&A plans to complete these efforts by December 31, 2024.

However, gathering data is only the first step, and to fully implement this recommendation, DHS needs to complete the in-depth assessment of the Open Source and Information Sharing processes. Completing the assessment will provide DHS I&A with information to address internal control deficiencies and help ensure that personnel consistently follow existing and updated policies for sharing information.

**Director:** Triana McNeil, Homeland Security and Justice

**Contact information:** McNeilT@gao.gov, (202) 512-8777

*Homeland Security: Office of Intelligence and Analysis Should Improve Privacy Oversight and Assessment of Its Effectiveness*. GAO-23-105475. Washington, D.C.: August 28, 2023.

**Year Recommendations Made:** 2023

**Recommendation:** The Under Secretary for Intelligence and Analysis should identify who is responsible for conducting the audits of information systems and bulk data described in I&A's Intelligence Oversight Guidelines, and to whom the results of these audits should be reported.

**Action Needed:** DHS concurred with this recommendation. DHS I&A planned for its Transparency and Oversight Program Office to coordinate with relevant I&A entities to develop a standard operating procedure for conducting audits of information systems and bulk data that would specify roles and responsibilities for these audits. In March 2024, DHS I&A officials reported delaying work on the procedure to prioritize work on other oversight-related activities. Consequently, officials pushed back the procedure's estimated date of completion from February to July 2024. Identifying entities responsible for conducting the audits and receiving the results will help I&A ensure implementation of oversight activities that have been required by its oversight guidelines since 2017 but were never performed.

**Recommendation:** The Under Secretary for Intelligence and Analysis should ensure that the responsible entities conduct audits of information systems and bulk data, as described in I&A's Intelligence Oversight Guidelines.

**Action Needed:** DHS concurred with this recommendation. As of March 2024, DHS planned to have the Director of I&A's Transparency and Oversight Program Office work with the entities responsible for conducting audits of information systems and bulk data to set a goal for the number of such audits to be conducted for the remainder of fiscal year 2024 and assess progress against that goal by the end of September 2024.

To fully implement this recommendation, I&A will need to complete the procedure identified in the previous recommendation to identify the entities responsible for conducting audits. Until I&A completes the procedure, I&A cannot ensure that the responsible entities have performed the required audits of information systems and bulk data.

**Director:** Triana McNeil, Homeland Security and Justice

**Contact information:** McNeilT@gao.gov, (202) 512-8777

**Information Technology and Cybersecurity**

*Coast Guard: Actions Needed to Enhance IT Program Implementation*. GAO-22-105092. Washington, D.C.: July 28, 2022.

**Year Recommendations Made:** 2022

**Recommendation:** The Commandant of the U.S. Coast Guard should direct the Deputy Commandant for Mission Support to implement the leading practices for network capacity planning that we identified, including (1) compiling a complete and accurate inventory of hardware, software, and configurations; (2) identifying traffic growth predictions; (3) prioritizing network traffic; (4) performing simulations and what-if-analyses; and (5) continually monitoring the health of the infrastructure to ensure it is meeting demand and mission needs.

**Action Needed:** DHS concurred with this recommendation. In April 2024, the Coast Guard stated that through its Infrastructure Managed Services contract, awarded in December 2022, the Coast Guard has required that its vendor address three of the five leading practices in the recommendation—compiling an inventory, prioritizing network traffic, and continually monitoring the health of the infrastructure. In addition, the Coast Guard stated that it plans to develop the supporting policies and requirements for the remaining two leading practices—identifying traffic growth predictions and performing simulations. The Coast Guard expected to have a timeline for completing this task by the end of fiscal year 2024. To fully implement the recommendation, the Coast Guard will need to demonstrate that it has established and implemented policies and practices that address each of the leading practices we identified for network capacity planning.

**Recommendation:** The Commandant of the U.S. Coast Guard should direct the Deputy Commandant for Mission Support to ensure that the plan or strategy for aligning all operational technology to the Department of Defense risk management framework is effectively implemented.

**Action Needed:** DHS concurred with this recommendation. In January 2024, Coast Guard stated that it plans to develop a standard to ensure that operational technology is securely configured in accordance with applicable Department of Defense policies and security controls. However, as of February 2024, the Coast Guard did not have an estimated timeframe for completing the standard.

To fully implement the recommendation, the Coast Guard will need to demonstrate that it has a plan to align its operational technology to the Department of Defense's risk management framework and has implemented that plan. By doing so, Coast Guard could be better positioned to manage cybersecurity risks to its operational technology.

**High Risk Area:** Improving the Management of IT Acquisitions and Operations

**Director:** Jennifer Franks, Information Technology and Cybersecurity
**Contact information:** FranksJ@gao.gov, (404) 679-1831
*Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks*. GAO-22-104256. Washington, D.C.: June 21, 2022.

**Year Recommendation Made:** 2022

**Recommendation:** The Director of the Cybersecurity and Infrastructure Security Agency should work with the Director of the Federal Insurance Office to produce a joint assessment for

Congress on the extent to which the risks to the nation's critical infrastructure from catastrophic cyberattacks, and the potential financial exposures resulting from these risks, warrant a federal insurance response.

**Action Needed:** DHS agreed with this recommendation. DHS has collaborated with the Department of the Treasury on identifying data needs for the agencies' joint assessment of the need for a federal insurance response to address catastrophic cyberattacks. As of March 2024, DHS plans to continue to collaborate with Treasury regarding a joint cyber insurance assessment.

To fully implement this recommendation, DHS needs to continue working with Treasury to engage with critical infrastructure sectors and produce a joint assessment for Congress, as DHS has indicated is its intent. An assessment with DHS's analysis of the cyber risks facing critical infrastructure could inform Congress in its deliberations related to addressing the increasing risk of catastrophic cyber incidents for U.S. critical infrastructure.

**High Risk Area:** Ensuring the Cybersecurity of the Nation

**Director:** Kevin Walsh, Information Technology and Cybersecurity
**Contact information:** WalshK@gao.gov, (202) 512-6151

*Biometric Identity System: DHS Needs to Address Significant Shortcomings in Program Management and Privacy.* GAO-23-105959. Washington, D.C.: September 12, 2023.

**Year Recommendation Made:** 2023

**Recommendation:** The Secretary of DHS should direct the OBIM Director to revise the schedule estimate for the HART program that incorporates the best practices called for in the GAO *Schedule Assessment Guide.*

**Action Needed:** DHS agreed with this recommendation. In February 2024, DHS officials stated that they are working on updating the HART program's schedule and incorporating GAO's scheduling best practices. The officials stated that they are aiming to complete this effort by the end of June 2024.

To fully implement this recommendation, DHS needs to finish revising the schedule. Once the program develops a reliable schedule, it will enable department leadership to make informed decisions regarding the program's future. It will also help program management officials mitigate future schedule slippages.

**High Risk Area:** Improving the Management of IT Acquisitions and Operations

**Director:** Kevin Walsh, Information Technology and Cybersecurity

**Contact information:** WalshK@gao.gov, (202) 512-6151

*Critical Infrastructure Protection: National Cybersecurity Strategy Needs to Address Information Sharing Performance Measures and Methods*. GAO-23-105468. Washington, D.C.: September 26, 2023.

**Year Recommendation Made:** 2023

**Recommendation:** The Director of CISA, in coordination with the 14 agencies, should conduct a comprehensive assessment of whether the current mix of centralized and federated sharing methods used by the agencies is the optimal approach to addressing the cyber threat sharing challenges—including whether existing sharing methods should be retired in favor of centralized or federated approaches.

**Action Needed:** DHS agreed with this recommendation. DHS stated that CISA would coordinate with the Office of the National Cyber Director (ONCD) to evaluate the feasibility of conducting a comprehensive assessment of existing information sharing methods. In February 2024, DHS explained that CISA had gained insight into the challenges and opportunities related to cybersecurity threat information sharing through extensive prior and ongoing engagement efforts with ONCD and federal agencies. As such, DHS stated that conducting a separate comprehensive assessment would be duplicative to those efforts. DHS added that CISA will work with ONCD to confirm whether those efforts provide the insights needed to address cyber threat information sharing challenges in an optimal manner and will make decisions about potential adjustments to related activities, as appropriate.

However, DHS has not yet documented the results of CISA's engagement efforts with ONCD and federal agencies. As such, it is unclear the extent to which those efforts provided full insight into whether the current mix of sharing methods is optimal for addressing the sharing challenges—including whether existing sharing methods should be retired. To fully implement this recommendation, DHS should complete and document its proposed comprehensive assessment to help determine whether existing sharing methods are optimal or whether any method should be retired.

**High Risk Area:** Ensuring the Cybersecurity of the Nation

**Director:** Marisol Cruz Cain, Information Technology and Cybersecurity

**Contact information:** CruzCainM@gao.gov, (202) 512-5017

**Director:** Tina Won Sherman, Homeland Security and Justice

**Contact information:** ShermanT@gao.gov, (202) 512-8777

*DHS Financial Management: Actions Needed to Improve Systems Modernization and Address Coast Guard Audit Issues*. GAO-23-105194. Washington, D.C.: February 28, 2023.

**Year Recommendations Made:** 2023

**Recommendation:** DHS's Under Secretary for Management should ensure that the JPMO works with Coast Guard to remediate known issues identified from testing, prior to declaring full operational capability for the ongoing financial systems modernization efforts.

**Action Needed:** DHS concurred with the recommendation. In April 2023, DHS officials approved a plan to remediate known issues identified from system testing (i.e., breach remediation plan). The plan included, among other things: (1) high-level root causes for the system performance issues or breach, (2) associated lessons learned, and (3) actions that JPMO will take to address the issues that were identified. According to DHS, its rebaselining efforts are ongoing. JPMO expects to address known issues and declare full operational capability in August 2025.

To fully implement this recommendation, DHS needs to fully implement its breach remediation plan, fully remediate the known issues, and declare full operational capability for Coast Guard's new financial management system.

**Recommendation:** DHS's Under Secretary for Management should ensure that the Joint Program Management Office works with FEMA to remediate issues as they arise from user testing prior to moving forward with subsequent milestones for the ongoing financial systems modernization efforts.

**Action Needed:** DHS concurred with the recommendation. DHS officials described actions they planned to take. Specifically, DHS stated that the JPMO will ensure that lessons learned from prior financial systems implementation translate into appropriate actions for the ongoing FEMA financial systems modernization efforts. DHS's overall estimated completion date for these actions is planned for September 30, 2024.

To fully implement this recommendation, FEMA needs to complete the discovery process to develop functional requirements for its new system and work with JPMO to help ensure that issues identified prior to the new system going live are remediated in a timely manner.

**Recommendation:** DHS's Under Secretary for Management should ensure that the Joint Program Management Office works with ICE to remediate issues as they arise from user testing prior to moving forward with subsequent milestones for the ongoing financial systems modernization efforts.

**Action Needed:** DHS concurred with the recommendation. DHS officials described actions they planned to take. Specifically, DHS stated that the JPMO will ensure that lessons learned from prior financial systems implementation translate into appropriate actions for the ongoing ICE financial systems modernization efforts. DHS's overall estimated completion date for these actions is planned for September 30, 2024.

To fully implement this recommendation, ICE needs to complete the discovery process to develop functional requirements for its new system and work with JPMO to help ensure that issues identified prior to the new system going live are remediated in a timely manner.

**High Risk Area:** Strengthening DHS IT and Financial Management Functions

**Director:** Paula Rascona, Financial Management and Assurance

**Contact information:** RasconaP@gao.gov, (202) 512-9816

**Chemical Security**

*Critical Infrastructure Protection: Actions Needed to Enhance DHS Oversight of Cybersecurity at High-Risk Chemical Facilities*. GAO-20-453. Washington, D.C.: May 14, 2020.

**Year Recommendation Made:** 2020

**Recommendation:** The Assistant Director of the Infrastructure Security Division should develop a workforce plan that addresses the program's cybersecurity-related needs, which should include an analysis of any gaps in the program's capacity and capability to perform its cybersecurity-related functions, and human capital strategies to address them.

**Action Needed:** DHS concurred with this recommendation. According to CISA officials, as of March 2023, they began collecting background and operational information to complete the workforce planning effort. However, on July 27, 2023, the statutory authority for the Chemical Facilities Anti-Terrorism Standards (CFATS) program—the program on which our

recommendations focused—expired. Therefore, further updates for this priority recommendation are pending reauthorization.

If the program is reauthorized, to fully address this recommendation, CISA needs to develop a workforce plan that includes analysis of any gaps in the chemical security program's capacity and capability to perform its cybersecurity-related functions, and human capital strategies to address them. Doing so will help the program ensure that it has the appropriate number of staff to carry out cybersecurity-related efforts.

**High Risk Area:** Ensuring the Cybersecurity of the Nation

**Director:** Tina Won Sherman, Homeland Security and Justice

**Contact information:** ShermanT@gao.gov, (202) 512-8777

**Infrastructure, Acquisitions, and Management**

*Federal Real Property: DHS and GSA Need to Strengthen the Management of DHS Headquarters Consolidation*. GAO-14-648. Washington, D.C.: September 19, 2014.

**Year Recommendation Made**: 2014

**Recommendation:** The Secretary of Homeland Security and the Administrator of the General Services Administration (GSA), after revising the DHS headquarters consolidation plans, should work jointly to develop revised cost and schedule estimates for the remaining portions of the consolidation project that conform to GSA guidance and leading practices for cost and schedule estimation, including an independent evaluation of the estimates.

**Action Needed:** DHS agreed with this recommendation (as did GSA). The Department of Homeland Security Headquarters Consolidation Accountability Act of 2015 required DHS to submit information to congressional committees regarding the current consolidation plan. The act required that DHS, in coordination with GSA, provide information that was consistent with what we recommended, including a comprehensive needs assessment, a costs and benefits analysis, and updated cost and schedule estimates.[32]

In March 2022, DHS—with input from GSA—submitted its report to congressional committees in response to the act. In August 2022, we found that this report did not contain sufficient information on the costs and schedules of the consolidation project's components for us to perform a comprehensive assessment based on GAO's leading practices in this area.

In July 2023, GSA provided us with a report on updated cost and schedule estimates for the project, and in December 2023, DHS provided us with updates for its estimates. As of February 2024, GSA and DHS provided documentation demonstrating some of our leading practices for the updated estimates.

To fully implement this recommendation, DHS and GSA need to provide additional documentation that demonstrates the updated cost and schedule estimates fully conform to our leading practices for cost and schedule estimation. Such estimates would support sound decision-making related to DHS's ongoing headquarters consolidation.

[32]Pub. L. No. 114-150, 130 Stat. 366 (2016).

**High Risk Area:** Managing Federal Real Property

**Director:** Christopher P. Currie, Homeland Security and Justice

**Contact information:** CurrieC@gao.gov, (202) 512-8777

**Director:** David Marroni, Physical Infrastructure

**Contact information:** MarroniD@gao.gov, (202) 512-2834

*Coast Guard: Actions Needed to Close Stations Identified as Overlapping and Unnecessarily Duplicative*. GAO-18-9. Washington, D.C.: October 26, 2017.

**Year Recommendation Made:** 2018

**Recommendation**: The Commandant of the Coast Guard should take action to close the stations identified according to its plan and target dates.

**Action Needed:** DHS agreed with this recommendation. DHS stated that it would begin implementing changes in the fall of 2018. According to Coast Guard officials, historically the closure process has been difficult due to factors such as concerns from affected communities and members of Congress. The Coast Guard has implemented a revised process, which includes notifications to Congress in its annual budget request and Federal Register notices to obtain public comments prior to taking action to close stations. As of April 2023, the Coast Guard reported that it had consolidated six of the 18 identified stations with larger adjacent stations. According to officials, the Coast Guard continues to evaluate future closures as of March 2024.

The Coast Guard has partially addressed this recommendation but continues to evaluate redundant stations for closure as part of its boat optimization process. The service plans to recommend additional closures of stations identified as redundant in future budget submissions, which we will continue to monitor. To fully implement this recommendation, DHS, through the Coast Guard, should close boat stations that provide overlapping search and rescue coverage and are unnecessarily duplicative, according to its plan and target dates.

**Potential Financial Benefit if Implemented:** Millions

**Director:** Heather MacLeod, Homeland Security and Justice

**Contact information:** MacleodH@gao.gov, (202) 512-8777

*Coast Guard Shore Infrastructure: Applying Leading Practices Could Help Better Manage Project Backlogs of at Least $2.6 Billion*. GAO-19-82. Washington, D.C.: February 21, 2019.

**Year Recommendation Made:** 2019

**Recommendation:** The Commandant of the Coast Guard should employ models for its asset lines for predicting the outcome of investments, analyzing trade-offs, and optimizing decisions among competing investments.

**Action Needed:** The Coast Guard agreed with the recommendation. As of March 2024, the Coast Guard had not employed models to evaluate its asset lines. Instead, the Coast Guard reported that it had identified a preferred solution, and estimated that it will complete this analysis and fully implement a modeling solution by the end of 2028. To fully implement this recommendation, the Coast Guard needs to employ its modeling solution for predicting the outcome of investments, analyzing trade-offs, and optimizing decisions among competing investments.

**Potential Financial Benefit if Implemented:** Millions

**Director:** Heather MacLeod, Homeland Security and Justice

**Contact information:** MacleodH@gao.gov, (202) 512-8777

*Coast Guard: Actions Needed to Evaluate the Effectiveness of Organizational Changes and Determine Workforce Needs*. GAO-20-223. Washington, D.C.: February 26, 2020.

**Year Recommendation Made:** 2020

**Recommendation:** The Commandant of the Coast Guard should update its April 2018 Manpower Requirements Plan to include time frames and milestones for completing manpower requirements analyses and determinations for all positions and units.

**Action Needed:** DHS concurred with this recommendation. In March 2023, the Coast Guard submitted an updated Manpower Requirements Plan to Congress. However, this plan did not include time frames and milestones for the Coast Guard to complete manpower requirements analyses and determinations for all positions and units, as we recommended. In this way, the Coast Guard's plan did not fully meet the intent of our recommendation.

In September 2023, Coast Guard officials provided a memorandum with a list of manpower studies the Coast Guard intends to conduct from fiscal years 2023 through 2028. According to the document, dated August 2023, the Coast Guard intends to begin or complete manpower requirements analysis for 21 unit types, subject to resource availability, shifting priorities, and other factors. However, these 21 unit types cover only 29 percent of the Coast Guard's workforce. As of February 2024, the Coast Guard completed manpower requirements determinations for three of the 21 unit types it identified.

To fully implement this recommendation the Coast Guard needs to create a plan with time frames and milestones for completing manpower requirements analyses and determinations for all of its positions and units. We will continue to monitor actions Coast Guard takes to fully implement this recommendation.

**Director:** Heather MacLeod, Homeland Security and Justice

**Contact information:** MacleodH@gao.gov, (202) 512-8777

*Coast Guard: Actions Needed to Improve National Vessel Documentation Center Operations*. GAO-21-100. Washington, D.C.: December 16, 2020.

**Year Recommendation Made:** 2021

**Recommendation:** The Commandant of the Coast Guard should direct the Assistant Commandant for Prevention Policy to ensure that the National Vessel Documentation Center (NVDC) conducts a full cost study of NVDC's commercial and recreational user fees.

**Action Needed:** DHS concurred with the recommendation. In concurring with this recommendation, the Coast Guard stated that the NVDC will conduct a full cost study of its commercial and recreational user fees, with oversight provided as needed by the Director of Operations Resource Management for the Deputy Commandant for Operations. DHS officials stated that the NVDC would do so after the Coast Guard develops a new information technology system to accurately assess the actual costs of providing services to the public, including new information technology support costs. The Coast Guard has delayed the full cost study and, as of February 2024, estimates completing it by March 2026. By fully implementing this recommendation, the Coast Guard will have more assurance that its fees accurately charge users for the costs of providing its services.

**Potential Financial Benefit if Implemented:** Millions

**Director:** Heather MacLeod, Homeland Security and Justice

**Contact information:** MacLeodH@gao.gov, (202) 512-8777

*DHS Employee Morale: Some Improvements Made, but Additional Actions Needed to Strengthen Employee Engagement*. GAO-21-204. Washington, D.C.: January 12, 2021.

**Year Recommendation Made:** 2021

**Recommendation:** The DHS Office of the Chief Human Capital Officer (OCHCO) should monitor components' implementation of the OPM action planning cycle to ensure the components review and assess the results of their actions to adjust, reprioritize, and identify new actions needed to improve employee engagement.

**Action Needed**: DHS agreed with the recommendation. In March 2021, OCHCO issued written employee engagement guidance for DHS components that includes mechanisms for OCHCO to monitor components' implementation of the OPM action planning cycle. DHS OCHCO reviewed components' 2023 engagement plans and assessed the extent to which components are reviewing and assessing the results of their employee engagement efforts.

Overall, most DHS components are reviewing and assessing the results of their 2021 action plans. However, ICE did not do so in its 2023 action plan. According to OCHCO's assessment, limited personnel and other resource constraints have presented challenges for implementing and evaluating ICE's planned actions and action plan since 2021. OCHCO noted that with additional time, ICE may be better positioned to address some of these issues by the 2024 mid-cycle update, which is in process as of June 2024.

To fully address this recommendation, ICE must review and assess the results of the items in its action plan to adjust, reprioritize, and identify new actions needed to improve employee engagement.

**High Risk Area:** Strategic Human Capital Management

**Director:** Christopher P. Currie, Homeland Security and Justice

**Contact information:** CurrieC@gao.gov, (202) 512-8777

*Federal Contracting: Senior Leaders Should Use Leading Companies' Key Practices to Improve Performance*. GAO-21-491. Washington, D.C.: July 27, 2021.

**Year Recommendation Made:** 2021

**Recommendation:** The Secretary of Homeland Security should ensure the DHS Chief Procurement Officer (CPO) uses a balanced set of performance metrics to manage the department's procurement organizations, including outcome-oriented metrics to measure (a) cost savings/avoidance, (b) timeliness of deliveries, (c) quality of deliverables, and (d) end-user satisfaction.

**Action Needed:** DHS did not concur with the recommendation. DHS stated that while the department supports the use of outcome-oriented metrics, it disagreed that the specific metrics included in our recommendation necessarily captured the most relevant aspects of procurement organizations' performance. However, DHS also stated the CPO office would review its current metrics to determine whether they appropriately measure outcomes. We agree DHS could identify additional outcome-oriented metrics that are tailored to its needs. We also continue to believe DHS should address the recommendation by using the four types of metrics we identified because the corporate procurement leaders we interviewed emphasized the importance of using these types of outcome-oriented metrics.

In June 2023, the CPO office provided evidence that it was using an outcome-oriented metric to measure cost savings/avoidance achieved through category management activities, which are intended to improve how agencies procure common goods and services. DHS officials provided an update in February 2024 showing that in fiscal year 2023 the department used category management activities for about 80 percent of its common goods and services expenditures ($18 billion of $22.5 billion) and had tracked savings of $502 million.

To address the timeliness of deliveries and quality of deliverables metrics, the CPO officials noted that by June 2024 they plan to review marginal and unsatisfactory data from the Contractor Performance Reporting System. This analysis will then determine what additional steps are needed. To address the end-user satisfaction metric, the CPO office stated it supplemented its Acquisition 360 data by surveying procurement personnel and stakeholders, including end-users, in order to improve the procurement experience for their workforce and end-users. CPO officials stated that if performance gaps related to end-user experiences are identified, they will work to develop metrics, as needed.

To fully close this recommendation, DHS will need to provide evidence that it has implemented all the performance metrics to manage the department's procurement organization. Using a balanced set of performance metrics, including both process- and outcome-oriented measures would help DHS better identify improvement opportunities, set priorities, and allocate resources.

**Potential Financial Benefit if Implemented:** A Hundred Million or More Annually

**Director:** William Russell, Contracting and National Security Acquisitions

**Contact information:** RussellW@gao.gov, (202) 512-4841

*Coast Guard Acquisitions: Offshore Patrol Cutter Program Needs Mature Technology and Design*. GAO-23-105805. Washington, D.C.: June 20, 2023.

**Year Recommendation Made:** 2023

**Recommendation:** The Commandant of the Coast Guard should ensure that the Offshore Patrol Cutter (OPC) stage 2 program achieves a sufficiently stable design prior to the start of lead ship construction. In line with shipbuilding leading practices, sufficiently stable design includes 100 percent completion of basic and functional design, including routing of major distributive systems and transitive components that effect multiple zones of the ship.

**Action Needed:** DHS did not concur with this recommendation. DHS stated that the design would be sufficiently stable but not 100 percent complete basic and functional design. We stand by this recommendation as it aligns with our leading practices in shipbuilding and a statutory requirement for Navy programs. In April 2024, the Coast Guard said that the construction of OPC 5 will start by September 2024.

To fully implement this recommendation, the Coast Guard should not start construction until basic and functional design are 100 percent complete. The Coast Guard can ensure that all basic and functional design drawings are fully complete with all vendor-furnished information, including those that pertain to distributive systems and transitive components that affect multiple zones of the ship. The Coast Guard can refrain from approving construction without the contractor fully completing the basic and functional design drawings.

**Director:** Shelby Oakley, Contracting and National Security Acquisitions

**Contact information:** OakleyS@gao.gov, (202) 512-4841

*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.

**Year Recommendation Made:** 2023

**Recommendation:** The DHS Secretary should ensure the DHS Under Secretary for Management ensures design for the lead Polar Security Cutter is mature, meaning at least the functional design is complete, including routing of major distributive systems that affect multiple zones of the ship, prior to authorizing lead cutter construction beyond the previously approved eight prototype units.

**Action Needed:** DHS concurred with this recommendation. DHS stated that the Department's goal for the Polar Security Cutter's design maturity is consistent with this recommendation—to complete functional design, including routing of major distributive systems that affect multiple zones of the ship prior to authorizing construction of the first ship. In January 2024, DHS said the DHS Management Directorate Office of Program Accountability and Risk Management was monitoring the progression of the design on a bimonthly basis and the estimated completion date is September 30, 2024.

To fully implement this recommendation, the Coast Guard should not start construction beyond the previously approved eight prototype units until the Department of Homeland Security approves the next upcoming decision point for the program at acquisition decision event 2C, of which design maturity will be a key consideration informing the decision.

**Director:** Shelby Oakley, Contracting and National Security Acquisitions

**Contact information:** OakleyS@gao.gov, (202) 512-4841