U.S. DEPARTMENT OF HOMELAND SECURITY

OFFICE OF INSPECTOR GENERAL

OIG-24-64 September 30, 2024

FINAL REPORT

Oversight Reports Identify Recurring Challenges with DHS Strategic Planning

OFFICE OF INSPECTOR GENERAL
U.S. Department of Homeland Security
Washington, DC 20528 | www.oig.dhs.gov

September 30, 2024

MEMORANDUM FOR: The Honorable Alejandro N. Mayorkas
Secretary
Department of Homeland Security

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

FROM: Joseph V. Cuffari, Ph.D.
Inspector General

GLENN E SKLAR Digitally signed by GLENN E SKLAR Date: 2024.09.28 21:28:40 -04'00' *for*

SUBJECT: *Oversight Reports Identify Recurring Challenges with DHS Strategic Planning*

Attached for your action is our final report, *Oversight Reports Identify Recurring Challenges with DHS Strategic Planning*. We incorporated the formal comments provided by your office.

The report contains two recommendations aimed at improving the Department's recurring challenges with its strategic planning efforts. Your office concurred with both recommendations.

Based on information provided in your response to the draft report, we consider recommendations 1 and 2 open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions. Please send your response or closure request to OIGAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please contact me with any questions, or your staff may contact Kristen Bernard, Deputy Inspector General, Audits, at (202) 981-6000.

Attachment

DHS OIG HIGHLIGHTS

Oversight Reports Identify Recurring Challenges with DHS Strategic Planning

September 30, 2024

Why We Did This Review

DHS' mission requires close coordination and collaboration across eight operational components, seven support components, and the Office of the Secretary to achieve the goals and objectives within the DHS Strategic Plan for FYs 2020–2024. We conducted this review to summarize outdated or expired DHS and component strategic guidance identified in prior DHS OIG and GAO reports and determine the reasons the guidance is outdated or expired.

What We Recommend

We made two recommendations to address the Department's recurring challenges with its strategic planning efforts.

For Further Information:
Contact our Office of Public Affairs at (202) 981-6000, or email us at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

What We Found

Our review of prior Department of Homeland Security Office of Inspector General and U.S. Government Accountability Office (GAO) oversight reports identified recurring challenges with DHS' strategic planning efforts. We previously reported that DHS and its components had not promptly updated strategic guidance (1) by mandated deadlines or (2) to reflect new information that would have a significant impact on the risk environment for which the strategic guidance was developed. In conducting this review of reports issued from fiscal years 2018 to 2022, we determined 7 prior DHS OIG reports and 7 prior GAO reports referenced 20 outdated or expired DHS strategic guidance documents.

Since the issuance of these oversight reports, DHS and its components have updated 9 of the 20 strategic guidance documents. However, 11 of the documents remain outdated or expired. Additionally, there is a risk that other strategic guidance documents within the Department may possibly be outdated or expired.

Requirements for updating these strategic guidance documents varied; and the documents were outdated or expired for different reasons, including leadership challenges, insufficient resources, and prioritization of other operational activities. The absence of updated strategic guidance increases the risk that DHS and its components make operational and budgetary decisions based on outdated or expired information, which may reduce their ability to address the most current and critical challenges.

Department Response

DHS concurred with our recommendations. We consider these recommendations open and resolved.

Table of Contents

Abbreviations

CBP	U.S. Customs and Border Protection
CISA	Cybersecurity and Infrastructure Security Agency
FEMA	Federal Emergency Management Agency
FIOP	Federal Interagency Operational Plan
GAO	U.S. Government Accountability Office
IT	Information Technology
NDAA	National Defense Authorization Act
NSM-22	National Security Memorandum 22
OMB	Office of Management and Budget
PLCY	DHS Office of Strategy, Policy, and Plans
PPD-21	Presidential Policy Directive 21
Pub. L.	Public Law
SIPP	DHS Office of Strategic Integration and Policy Planning
TSA	Transportation Security Agency

Background

The Department of Homeland Security's mission is to safeguard the American people, our Homeland, and our values. This requires close coordination and collaboration across eight operational components, seven support components, and the Office of the Secretary to achieve the strategic goals and execute the strategic objectives within the DHS Strategic Plan for fiscal years 2020–2024. Per Office of Management and Budget (OMB) Circular No. A-11 Section 230 – *Agency Strategic Planning*, strategic plans "define the agency mission, long-term goals and objectives to achieve those goals, strategies planned, and approaches it will use to monitor its progress in addressing specific national problems, needs, challenges, and opportunities related to its mission."

Strategic planning is important because it helps DHS, and its components, prioritize efforts; effectively allocate resources; execute strategic goals; and provide a single, forward-focused vision that can align with the Department's mission. Further, various laws, regulations, directives, and policies require DHS and its components to develop and update strategic guidance. Primarily, the *GPRA Modernization Act of 2010*[1] requires Federal agencies to issue a strategic plan concurrent with the President's Budget at least every 4 years. Strategic planning allows agencies to align goals and objectives to resources and guides decision making to accomplish priorities and improve outcomes. Although the *GPRA Modernization Act of 2010* does not specifically address requirements for sub-level, component strategic plans, it serves as a framework for conducting long-range planning to achieve desired outcomes.

Subsequent legislative mandates and DHS Directive(s) affirm the need for coordinated policies and plans. For example:

- Section 709 of the *National Defense Authorization Act for Fiscal Year 2017* (NDAA FY 2017), states the DHS Under Secretary for Strategy, Policy, and Plans shall ''develop and coordinate policies to promote and ensure quality, consistency, and integration for the programs, components, offices, and activities across the Department."

- NDAA FY 2017 requires coordination by Department components to "ensure consistency with the policy priorities of the Department, the head of each component of the Department shall coordinate with the Office of Strategy, Policy, and Plans (PLCY) in establishing or modifying policies or strategic planning guidance with respect to each such component."

- DHS Management Directive 101-01, Revision 01, *Planning, Programming, Budgeting, and Execution*, June 2019, requires strategic planning goals and priorities to support funding

[1] Pub. L. 111-352. GPRA stands for the *Government Performance and Results Act of 1993* (Pub. L. 103-62).

decisions, operational execution, and measuring effectiveness to optimize results. The Directive requires PLCY to lead the Department's strategy development. See Appendix A for a list of the documents we reviewed.

During FYs 2018 through 2022, the DHS Office of Inspector General and the U.S. Government Accountability Office (GAO) issued seven reports each, referencing outdated or expired DHS and component strategic guidance documents. See Appendix C for a list of the 14 reports and strategic guidance documents. Hereafter, we will use "outdated" in place of "outdated or expired." These reports identified 20 outdated strategic guidance documents at DHS Headquarters, the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Emergency Management Agency (FEMA), the Transportation Security Administration (TSA), and U.S. Customs and Border Protection (CBP).

- CISA is responsible for leading and coordinating national security and resilience efforts for protecting the Nation's cyber systems and critical infrastructure against significant risks.
- FEMA coordinates Federal Government activities to prepare for, prevent, respond to, recover, and protect the Nation from natural or manmade disasters and acts of terrorism.
- TSA protects the Nation's transportation systems to secure freedom of movement for people and commerce.
- CBP safeguards the Nation's borders by keeping terrorists, their weapons, and dangerous people and illicit materials out of the United States while facilitating lawful international travel and trade.

We conducted this review to summarize outdated or expired DHS and component strategic guidance identified in prior DHS OIG and GAO reports and determine the reasons the guidance is outdated or expired.

Results of Review

Our review of prior DHS OIG and GAO oversight reports identified recurring challenges with DHS' strategic planning efforts. DHS OIG and GAO previously reported that DHS and its components had not promptly updated strategic guidance (1) by mandated deadlines or (2) to reflect new information that would have a significant impact on the risk environment for which the strategic guidance was developed. In conducting this review of reports issued from FYs 2018 to 2022, we determined 7 prior DHS OIG reports and 7 prior GAO reports referenced 20 outdated DHS strategic guidance documents.

Since the issuance of these oversight reports, DHS and its components have updated 9 of the 20 strategic guidance documents. However, 11 of the documents remain outdated. This includes one we determined DHS should update, despite the fact there is no statutory requirement to do

so. Additionally, there is a risk that other strategic guidance documents within the Department may possibly be outdated.

Requirements for updating these strategic guidance documents varied; and the documents were outdated for different reasons, including leadership challenges, insufficient resources, and prioritization of other operational activities. Consequently, in all cases, the absence of updated strategic guidance increases the risk that DHS and its components make operational and budgetary decisions based on outdated information, which may reduce their ability to address the most current and critical challenges.

Recurring Challenges with DHS Strategic Planning Efforts

Our review of prior DHS OIG and GAO reports identified recurring challenges with the Department's strategic planning efforts. Specifically, during FYs 2018 through 2022, 14 DHS OIG and GAO reports referenced 20 outdated strategic guidance documents that had not been promptly updated by DHS and its components (1) by mandated deadlines or (2) to reflect new information that would have a significant impact on the risk environment for which the strategic guidance was developed. See Table 1 for the total number of outdated strategic guidance documents identified in DHS OIG and GAO reports, as well as the number of these that remain outdated or have been updated as of May 2024.

Table 1. Outdated Strategic Guidance Documents Identified in DHS OIG and GAO Reports

Agency	Total Number	Remain Outdated	Subsequently Updated
DHS	3	1	2
CBP	1	0	1
CISA	7	7[2]	0
FEMA	8	3	5
TSA	1	0	1
Totals	**20**	**11**	**9**

Source: DHS OIG analysis based on reviews of DHS OIG and GAO reports from FYs 2018 to 2022

Absence of Updated Strategic Guidance in Key Departmental Activities

DHS OIG and GAO reports identified outdated strategic guidance affecting key mission areas of DHS and its components. For example:

[2] CISA leads coordination for the review and approval of all modifications for six of the outdated strategic guidance documents. The Department of Energy manages the other outdated strategic guidance document but collaborates with CISA in developing and updating it.

- **DHS:** DHS had not updated three important strategic guidance documents, including the Quadrennial Homeland Security Review, which identifies the Department's critical homeland security missions and its strategy for meeting them.

- **CISA:** CISA had not updated seven strategic guidance documents, including the National Infrastructure Protection Plan (National Plan), which guides the national effort to manage risk to the Nation's critical infrastructure from significant threats and hazards to physical and cyber critical infrastructure. Specifically, the National Plan had not been updated since 2013, or for nearly 8 years. CISA also had not updated plans for the protection of six critical infrastructure sectors and subsectors, including Dams, Energy, Government Facilities, Communications, Commercial Facilities, and Election Infrastructure.[3]

- **FEMA:** FEMA had not updated eight strategic guidance documents related to its emergency management mission. One of these documents was its National Disaster Recovery Framework, which FEMA had not updated since 2016. This framework provides guidance on building, sustaining, and coordinating delivery of recovery capabilities for stakeholders such as Federal, state, tribal, and territorial governments; private sector entities; and individuals. Additionally, FEMA was behind in updating Federal Interagency Operational Plans (FIOP) for three response and recovery mission areas.

Requirements for Updating Department Strategic Guidance Documents

Requirements for updating these strategic guidance documents varied. In many cases, laws, policies, or internal guidance mandated DHS and its components update these strategic guidance documents on a regular, recurring basis. For example, section 707 of the *Homeland Security Act of 2002* requires DHS to conduct and publish the Quadrennial Homeland Security Review every 4 years.[4] In other cases, although there were no specific mandates for regular, recurring updates, DHS OIG and GAO identified the need to update the plans due to changes

[3] Our analysis only identified six outdated critical infrastructure sector and subsector-specific plans. However, DHS is the sector risk management agency responsible for eight sectors — Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Emergency Services; Information Technology; and Nuclear Reactors, Materials, and Waste. DHS is jointly responsible for Government Facilities and Transportation Systems. The Department of Energy is responsible for the Energy Sector, but DHS plays a role, and the Election Subsector is under the Government Facilities Sector.

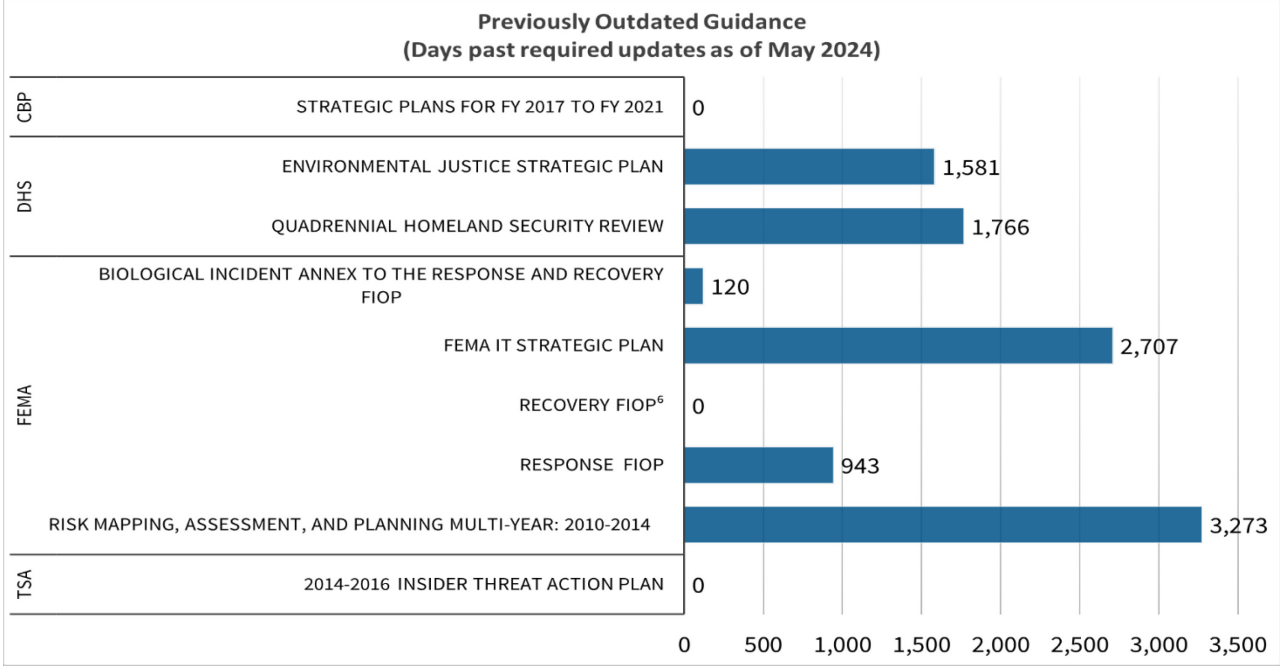
[4] Section 707 of the *Homeland Security Act of 2002*, as amended by the *Implementing Recommendations of the 9/11 Commission Act of 2007*, requires that beginning in FY 2009 and every 4 years thereafter, DHS conduct a review that provides a comprehensive examination of the homeland security strategy of the United States (referred as a "quadrennial homeland security review") including recommendations regarding the long-term strategy and priorities of the Nation for homeland security and guidance on the programs, assets, capabilities, budget, policies, and authorities of the Department.

within the Department's operating environment. For instance, TSA's Insider Threat Action Plan[5] does not have specific update requirements, but GAO recommended TSA develop a new strategic plan for its Insider Threat Program to reflect the program's current goals, objectives, and priorities.

Progress Made by DHS and Components in Updating Strategic Guidance Documents

Since issuance of the DHS OIG and GAO reports, DHS and its components have updated 9 of the 20 outdated strategic guidance documents. Of note, FEMA's Risk Mapping, Assessment, and Planning Multi-Year Plan was outdated for 3,273 days, or approximately 9 years, before FEMA updated it. Similarly, FEMA's Information Technology (IT) Strategic Plan was outdated for 2,707 days, or approximately 7 years, before its latest update. Figure 1 identifies the nine strategic documents that DHS and its components have updated and the number of days the documents had been outdated prior to their updates.

Figure 1. Outdated Strategic Guidance Subsequently Updated



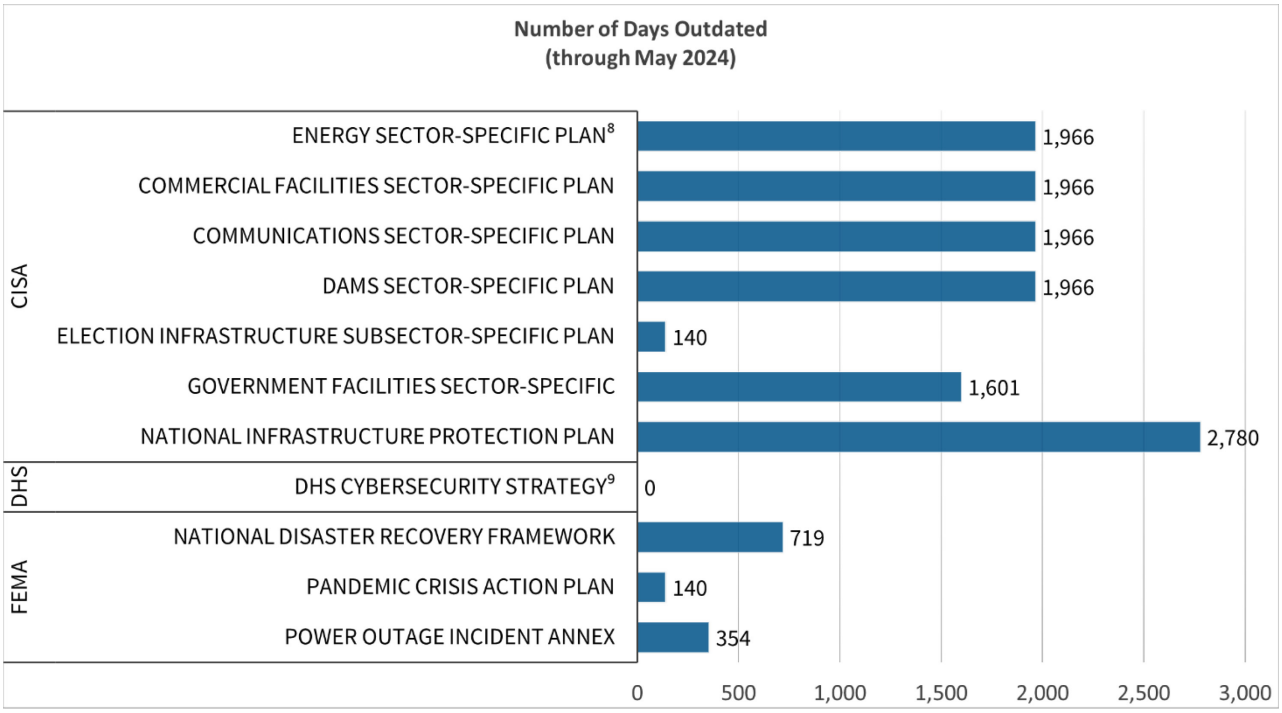
Source: DHS OIG calculation based on the dates strategic guidance was required to be updated and when updates occurred[6]

[5] In 2013, TSA developed a 2014–2016 Insider Threat Action Plan, which outlined TSA's strategic vision and goals for its Insider Threat Program.

[6] Per the 2016 version of the Recovery FIOP, FEMA should update the Recovery FIOP "periodically, as required, to incorporate new executive guidance and statutory and procedural changes, as well as lessons learned from exercises and actual incidents." However, the document does not specify a required interval for these updates.

Despite this progress, as of May 2024, DHS and its components have yet to update 11 remaining strategic guidance documents, including one we determined DHS should update even though there are no statutory requirements to do so.[7] Of particular concern, CISA's National Plan has been outdated for 2,780 days, or nearly 8 years, as of May 2024. Figure 2 shows the DHS and component strategic guidance documents that remain outdated as of May 2024. Appendix D and Appendix E contain additional information about CISA and FEMA's outdated strategic guidance documents.

Figure 2. Currently Outdated Strategic Guidance Documents



[8, 9]

Source: DHS OIG calculation based on the date when strategic guidance documents were identified as outdated and the end of DHS OIG's review period in May 2024

[7] Although there is no legal mandate to update the 2018 DHS Cybersecurity Strategy, the Department should periodically update this framework to keep pace with the evolving cyber risk landscape and the execution of its cybersecurity responsibilities.

[8] The Department of Energy is the Sector Risk Management Agency for the Energy Sector, but coordinates with DHS, through CISA, to update the Energy Sector-Specific Plan.

[9] Per the 2018 Cybersecurity Strategy, DHS planned to review and update this strategy in 2023 and periodically thereafter. However, in October 2023, PLCY affirmed that there were no plans to update the 2018 Cybersecurity Strategy, although those plans could change.

Delays in Updating Strategic Guidance Due to a Variety of Reasons

These strategic guidance documents were or remain outdated for different reasons, including leadership challenges, insufficient resources, and prioritization of other operational activities. For example:

- FEMA prioritized its response to the COVID-19 pandemic, which delayed updates for six of the strategic guidance documents within its National Preparedness System.[10]

- Challenges with leadership, insufficient resources, and other factors postponed updates to two outdated strategic guidance documents from FEMA and one from TSA.

- DHS did not provide an explanation to OIG regarding why the Department had not updated two of its documents.

- DHS and CBP's U.S. Border Patrol each had one outdated strategic guidance document that did not have statutory update requirements. Although there was no statutory update requirement, we reported in OIG-19-24, *Progress Made, But Additional Efforts Are Needed to Secure the Election Infrastructure*, the need to update the DHS strategic guidance for operational purposes. Additionally, according to CBP, its strategic guidance was subsequently required to be updated by Executive Order.

In 2022, the National Security Council directed CISA to pause a refresh of the National Plan pending an update to Presidential Policy Directive 21 (PPD-21), *Critical Infrastructure Security and Resilience*.[11] However, at that time, the National Plan was already outdated because it had not been revised since 2013, or in nearly 8 years. CISA affirmed this pause also affected six other plans that were dependent on the National Plan. On April 30, 2024, the President signed the *National Security Memorandum on Critical Infrastructure Security and Resilience* (NSM-22), rescinding and replacing PPD-21. CISA expects to update the six sector-specific plans by January 24, 2025, and then the National Plan by April 30, 2025, as required by NSM-22.[12]

Table 2 summarizes the various reasons why DHS and its components stated they did not update their strategic guidance documents in a timely manner.

---

[10] FEMA's National Preparedness System outlines an organized process to achieve the National Preparedness Goal, which identifies a wide range of threats and hazards that continue to pose a significant risk to the Nation, such as natural hazards, pandemics, terrorist attacks, and malicious cyber activities.

[11] PPD-21, dated February 12, 2013, established national policy on critical infrastructure security and resilience; clarified critical infrastructure-related functions, roles, and responsibilities across the Federal Government; and enhanced overall coordination and collaboration.

[12] NSM-22 requires each Sector Risk Management Agency to submit its sector-specific risk management plan to DHS within 270 days of the enactment of NSM-22 (April 30, 2024). NSM-22 also requires DHS to submit the National Plan within 1 year of the enactment of NSM-22.

Table 2. Reasons for Delay in Strategic Guidance Document Updates

Reason	DHS	CISA	CBP	FEMA	TSA
Pending Federal Guidance	-	✓	-	-	-
COVID-19 Pandemic	-	-	-	✓	-
Leadership and Other Challenges	-	-	-	✓	✓
No Explanation	✓	-	-	-	-
No Requirement to Update	✓	-	✓	-	-

- No data
✓ Positive response

Source: DHS OIG analysis of DHS and components' questionnaire responses

Effects of Outdated Guidance

The absence of updated strategic guidance increases the risk that DHS and its components make operational and budgetary decisions based on outdated information, which may reduce their ability to address the most current and critical challenges. For example, in OIG-19-58, *FEMA's Longstanding IT Deficiencies Hindered 2017 Response and Recovery Operations*, we noted without an IT strategic plan, architecture, or centralized governance approach to guide effective IT decision making, FEMA exceeded its $452 million approved IT budget by approximately $56 million.

Additionally, there is a risk that DHS and its components have other outdated strategic guidance not identified in DHS OIG and GAO reports. For example, the 2013 National Plan provided strategic direction for 16 critical infrastructure sectors, including the 6 sectors identified as having outdated guidance in DHS OIG and GAO reports. The National Plan required each sector to develop a sector-specific plan, and update it "every four years thereafter," to support the national goals for critical infrastructure security and resilience at the sector level. Therefore, there is a potential risk that sector-specific plans for other critical infrastructure sectors not managed by DHS are also not current, and DHS and its Federal partners are making operational decisions based on outdated guidance.

Conclusion

Based on our review of prior DHS OIG and GAO reports, we concluded that DHS and its components' noncompliance with required strategic guidance document updates were not isolated incidents. Instead, the noncompliance appears to point to recurring challenges with DHS strategic planning. Additional oversight of strategic planning for DHS and its components is necessary to ensure timely updates and alignment with current Department policies and

guidance. Our review was limited to DHS OIG and GAO reports that identified outdated strategic guidance from FYs 2018 through 2022. We may not have identified and included other outdated DHS and component strategic guidance in our scope. This risk can be lowered by having PLCY, which is already required to manage the Department's strategic plans by DHS Management Directive 101-01, also oversee component strategic planning.

Recommendations

Recommendation 1: We recommend the Secretary direct the Office of Strategy, Policy, and Plans to ensure the timely development and updates of Department and component strategic guidance.

Recommendation 2: We recommend the Under Secretary for Strategy, Policy, and Plans:

- conduct an inventory of all required Department and component strategic guidance documents and mandated updates; and
- implement and track the updates to all strategic guidance documents, and ensure they remain current.

Management Comments and OIG Analysis

DHS provided management comments on a draft of this report. We included the comments in their entirety in Appendix B. We also received technical comments from DHS on the draft report, and we revised the report as appropriate. FEMA did not provide technical comments. DHS concurred with both recommendations, which we consider open and resolved. A summary of the Department's responses to the recommendations and our analysis follows.

DHS Response to Recommendation 1: Concur. The Office of Strategic Integration and Policy Planning (SIPP) already develops and coordinates policies to promote and ensure quality, consistency, and integration of perspectives from programs, components, offices, and activities with equities in these policies from across the Department. This is done through, among other means, the DHS Strategic Plan and the Quadrennial Homeland Security Review.

As components ensure consistency with the policy priorities of the Department, SIPP will coordinate with the head of each component's strategy team to establish or modify policies and strategic planning guidance impacting each component, as appropriate. Additionally, PLCY will consider which forum, or forums, would be most appropriate to facilitate communication and coordination across the Department regarding strategic guidance documents and efforts. Estimated completion date: February 28, 2025.

OIG Analysis: We consider PLCY's actions responsive to the recommendation, which is open and resolved. The recommendation will remain open until SIPP coordinates with the head of each component's strategy team to establish or modify policies to ensure timely development and updates of Department and component strategic guidance. Additionally, PLCY must establish the appropriate forum or forums to facilitate communication and coordination across the Department regarding strategic guidance documents and efforts.

DHS Response to Recommendation 2: Concur. Although SIPP already conducts periodic inventories of Department and component strategic guidance documents, the Department clarified that PLCY does not implement updates to all strategic guidance documents, as it is the responsibility of components to ensure consistency with the policy priorities of the Department. However, SIPP will coordinate with component strategy teams across DHS to establish or modify policies or strategic planning guidance, as appropriate, and develop a mechanism to track the latest strategic publications and any publications scheduled to be published across the Department. Estimated completion date: February 28, 2025.

OIG Analysis: We consider PLCY's actions responsive to the recommendation, which is open and resolved. The recommendation will remain open until SIPP provides its process for periodic inventory of Department and component strategic guidance documents, coordinates with component strategy teams to establish or modify policies or strategic planning guidance, and develops a mechanism to track all strategic guidance documents and ensure they remain current.

Appendix A:
Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Pub. L. No. 107−296) by amendment to the *Inspector General Act of 1978*.

The objective of this review was to summarize outdated or expired DHS and component strategic guidance identified in prior DHS OIG and GAO reports and determine the reasons the guidance is outdated or expired. Our scope was DHS OIG and GAO reports issued during FYs 2018 through 2022.

To answer our objective, we reviewed DHS OIG audit, inspection, and evaluation reports issued during FYs 2018 through 2022. We also reviewed GAO reports and testimonies related to DHS that contained the word "strategic" and were issued between October 1, 2017, and September 30, 2022. We downloaded and reviewed 390 DHS OIG reports and 210 GAO reports to determine whether they referenced outdated DHS or component strategic guidance.

We identified seven DHS OIG reports and seven GAO reports that referenced outdated DHS or component strategic guidance. We reviewed these reports to identify laws, regulations, etc., requiring updates to the outdated guidance and recommendations regarding the outdated guidance.

We gathered recommendation data for each DHS OIG report from DHS OIG's official system of record, Project Tracking System, and for each GAO report from GAO's website and reviewed this data to determine the status of the recommendations made in these reports. To assess the reliability of the Project Tracking System–generated data and GAO recommendation data, we traced the recommendations to the relevant report language to determine if information was entered into the system correctly. We organized the guidance in lists according to whether DHS OIG or GAO reported it as outdated and according to whether the recommendations remain open or have been closed.

To determine the reasons the guidance is or was outdated, we issued questionnaires to DHS Headquarters and the components — CISA, CBP, TSA, and FEMA — responsible for strategic guidance identified as outdated in DHS OIG or GAO reports and reviewed their responses. DHS and the components completed and returned all questionnaires. We provided questionnaires to DHS Headquarters and 21 components and offices to determine, among other things, if they are required to develop and update strategic guidance and how they define "strategic guidance." All 22 questionnaires were completed and returned to us for our analysis.

We obtained and analyzed the 2013 National Plan and the following laws, regulations, directives, and policies to identify requirements for DHS and components to develop strategic guidance:

1. Pub. L. 114-328, *National Defense Authorization Act for FY 2017*, December 2016
2. Pub. L. 111-352, *GPRA Modernization Act of 2010*, January 2011
3. Pub. L. 107-296, *Homeland Security Act of 2002*, November 2002
4. White House Press Release dated February 12, 2013, discussing PPD-21, *Critical Infrastructure Security and Resilience*
5. OMB Circular A-11, *Preparation, Submission and Execution of the Budget*, August 2022
6. Pub. L. 114-285, *Federal Law Enforcement Training Centers Reform and Improvement Act of 2015*, December 2016
7. Pub. L. 116-116, *DHS Field Engagement Accountability Act of 2020*, March 2020
8. 49 United States Code § 114(s)
9. Pub. L. 116-6, *Consolidated Appropriations Act, 2019*, February 2019
10. Senate Report 115-283 accompanying the *Consolidated Appropriations Act, 2019*, June 2018
11. Pub. L. 117-103, *Consolidated Appropriations Act, 2022*, March 2022
12. Explanatory Statement for the Homeland Security Appropriations Bill, 2022
13. Pub. L. 113-245, *Transportation Security Acquisition Reform Act*, December 2014
14. White House Press Release dated February 12, 2013, discussing Executive Order 13636, Improving *Critical Infrastructure Cybersecurity*
15. DHS web page describing National Security Presidential Directive-47/Homeland Security Presidential Directive-16
16. Pub. L. 110-53, *Implementing Recommendations of the 9/11 Act*, August 2007
17. OMB Circular A-130, *Managing Information as a Strategic Resource*
18. Executive Order 12898, *Federal Actions to Address Environmental Justice in Minority Populations and Low-Income Populations*, February 1994
19. Pub. L. 115-278, *Cybersecurity and Infrastructure Security Agency Act of 2018*, November 2018
20. Pub. L. 116-283, *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*, January 2021
21. DHS Delegation to the Under Secretary for Strategy, Policy, and Plans, DHS Delegation Number: 23000 – Revision Number 01, January 2022
22. DHS Directive 101-01, *Planning, Programming, Budgeting and Execution*, Revision 01, June 2019
23. DHS Policy Instruction IA-301, *DHS Intelligence and Analysis Planning, Programming, Budgeting, and Evaluation*, Revision 00, November 2013 – For Official Use Only
24. DHS Directive 142-02, *Information Technology Integration and Management*, Revision Number 01, April 2018
25. FEMA Instruction FI-112-23-001, *Planning, Programming, Budgeting, Execution (PPBE) – Planning Phase*, Version 1.0, May 2023

26. White House Press Release dated April 30, 2024, discussing *National Security Memorandum: Critical Infrastructure Security and Resilience*

To assess the reliability of information obtained for this review, we evaluated DHS and component definitions of strategic guidance and corroborated them using strategic guidance documents and definitions from GAO and OMB. We reviewed reports issued by DHS OIG and GAO and reviewed status reports for the relevant recommendations made in these reports. We corroborated DHS and components' responses by reviewing relevant laws and regulations. We interviewed PLCY officials to discuss their interpretations of the NDAA FY 2017, which required components to coordinate with DHS when establishing or modifying strategic planning guidance. We also corroborated the reasonableness of PLCY's interpretation with our Office of Counsel. Therefore, we determined the information we obtained is sufficiently reliable for the purposes of our review.

We conducted this review between May 2023 and May 2024 under the authority of the *Inspector General Act of 1978*, 5 United States Code §§ 401–424, and according to the *Quality Standards for Inspections and Evaluations*, issued by the Council of the Inspectors General on Integrity and Efficiency. Those standards require that evidence must sufficiently and appropriately support inspection findings and provide a reasonable basis for conclusions. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our review objective.

DHS OIG's Access to DHS Information

During this review, DHS and its components provided timely responses to our requests for information and did not delay or deny access to information we requested.

Appendix B:
DHS Comments on the Draft Report

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

Homeland Security

BY ELECTRONIC SUBMISSION

September 20, 2024

MEMORANDUM FOR: Joseph V. Cuffari, Ph.D.
Inspector General

FROM: Jim H. Crumpacker JIM H CRUMPACKER Digitally signed by JIM H CRUMPACKER Date: 2024.09.20 14:40:59 -04'00'
Director
Departmental GAO-OIG Liaison Office

SUBJECT: Management Response to Draft Report: Oversight Reports Identify Recurring Challenges with DHS Strategic Planning (Project No. 23-026-AUD-DHS)

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS, or the Department) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

DHS leadership is pleased to note OIG's recognition of efforts to update nine Component strategic guidance documents since issuance of DHS OIG and U.S. Government Accountability Office reports issued during fiscal year 2018 through 2022. OIG also acknowledged the importance of strategic planning, which helps DHS and Components prioritize efforts; effectively allocate resources; execute strategic goals; and provide a single, forward-focused vision that can align with the Department's mission. DHS remains committed to strengthening processes for updating strategic guidance to articulate the Department's missions and goals, the strategies we employ to achieve each goal, and long-term performance measures that we use to evaluate our progress.

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

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions.

Attachment

Attachment: Management Response to Recommendations Contained in 23-026-AUD-DHS

OIG recommended that the Secretary direct the Office of Strategy, Policy, and Plans (PLCY):

Recommendation 1: Ensure the timely development and updates of Department and component strategic guidance.

Response: Concur. The Office of Strategic Integration and Policy Planning (SIPP) already develops and coordinates policies to promote and ensure quality, consistency, and integration of perspectives from programs, Components, offices, and activities with equities in these policies form across the Department. This is done through, among other means, the DHS Strategic Plan[1] and the Quadrennial Homeland Security Review.[2]

However, PLCY also recognizes the importance of strengthening efforts to ensure the timely development and updates of Department and Component strategic guidance. As Components ensure consistency with the policy priorities of the Department, SIPP will coordinate with the head of each Component's strategy team to establish or modify policies and strategic planning guidance, impacting each Component, as appropriate. Additionally, PLCY will consider which forum, or forums, would be most appropriate to facilitate communication and coordination across the Department regarding strategic guidance documents and efforts.

Estimated Completion Date (ECD): February 28, 2025.

Recommendation 2:

- Conduct an inventory of all required Department and component strategic guidance documents and mandated updates; and
- Implement and track the updates to all strategic guidance documents, and ensure they remain current.

Response: Concur. Although SIPP already conducts periodic inventories of Department and Component strategic guidance documents, it is important to clarify that PLCY does not implement updates to all strategic guidance documents, as it is the responsibility of Components to ensure consistency with the policy priorities of the Department. However, SIPP will coordinate with Component strategy teams of across DHS to

[1] "Department of Homeland Security's Strategic Plan for Fiscal Years 2020-2024," https://www.dhs.gov/publication/department-homeland-securitys-strategic-plan-fiscal-years-2020-2024
[2] "Quadrennial Homeland Security Review," 2023 version dated April 2023; https://www.dhs.gov/quadrennial-homeland-security-review

establish or modify policies or strategic planning guidance, as appropriate, and develop a mechanism to track the latest strategic publications and scheduled to be published across the Department.

ECD: February 28, 2025.

Appendix C:
DHS OIG and GAO Reports Identifying Outdated Strategic Guidance, the Guidance, Mandate or Reason for Necessary Update, and Status of the Guidance, as of May 2024

Report Number	Responsible Component	Strategic Guidance Identified as Outdated	Mandate or Reason for Necessary Update	Remains Outdated	Updated
1. OIG-19-24	CISA	National Plan	PPD-21/NSM-22[13]	X	-
	CISA	Government Facilities Sector-Specific Plan	National Plan/NSM-22	X	-
	DHS	DHS Cybersecurity Strategy[14]	The 2018 DHS Cybersecurity Strategy did not include the Election Infrastructure Subsector	X	-
2. OIG-20-37	CISA	National Plan (previously identified)	PPD-21/NSM-22	X	-
	CISA	Commercial Facilities Sector-Specific Plan	National Plan/NSM-22	X	-
3. OIG-21-01	CISA	National Plan (previously identified)	PPD-21/NSM-22	X	-
	CISA	Government Facilities Sector-Specific Plan (previously identified)	National Plan/NSM-22	X	-
	CISA	Election Infrastructure Subsector-Specific Plan	National Plan/NSM-22	X	-
4. OIG-21-59	CISA	National Plan (previously identified)	PPD-21/NSM-22	X	-
	CISA	Dams Sector-Specific Plan	National Plan/NSM-22	X	-
5. OIG-22-63	Department of Energy	Energy Sector-Specific Plan (Dept. of Energy is responsible for this plan but cannot update it until the	National Plan/NSM-22	X	-

[13] Before the issuance of NSM-22 on April 30, 2024, PPD-21 required DHS to update the National Plan.
[14] According to PLCY, only a one-time strategy was required and there is no statutory requirement to update this strategy.

Report Number	Responsible Component	Strategic Guidance Identified as Outdated	Mandate or Reason for Necessary Update	Remains Outdated	Updated
		National Plan is updated)			
	FEMA	National Disaster Recovery Framework	FEMA Directive 112-12	X	-
	FEMA	Response FIOP	Internal Component Guidance	-	X
	FEMA	Recovery FIOP	Internal Component Guidance	-	X
	FEMA	Power Outage Incident Annex Plan	FEMA Directive 112-12	X	-
6. GAO-22-104462	CISA	Communications Sector-Specific Plan	National Plan/NSM-22	X	-
7. GAO-22-104279	CISA	National Plan (previously identified)	PPD-21/NSM-22	X	-
8. OIG-21-64	FEMA	Biological Incident Annex to the Response and Recovery FIOPs	FEMA Directive 112-12	-	X
	FEMA	Pandemic Crisis Action Plan	FEMA Directive 112-12	X	-
9. OIG-19-58	FEMA	Information Technology Strategic Plan	Government Performance and Results Act Modernization Act of 2010	-	X
10. GAO-22-104079	FEMA	Risk Mapping, Assessment, and Planning Multi-Year Plan for FYs 2010 through 2014	Department of Homeland Security Appropriations Act for FY 2009	-	X
11. GAO-19-543	DHS	Environmental Justice Strategic Plan	2011 Memorandum of Understanding on Environmental Justice	-	X
12. GAO-18-62	DHS	Quadrennial Homeland Security Review[15]	Section 707 of the *Homeland Security Act of 2002*	-	X

[15] The third Quadrennial Homeland Security Review was scheduled to be released in 2018 but was not released until April 2023.

Report Number	Responsible Component	Strategic Guidance Identified as Outdated	Mandate or Reason for Necessary Update	Remains Outdated	Updated
13. GAO-20-275	TSA	2014-2016 Insider Threat Action Plan	TSA's Insider Action Plan did not reflect current goals and objectives	-	X
14. GAO-18-11	CBP	U.S. Border Patrol Strategic Plan	Not Applicable[16]	-	X

- No data
X Positive response

Source: DHS OIG analysis of the listed reports

[16] According to CBP, there is "no statutory or agency regulation that requires strategic guidance from components below the agency level." However, U.S. Border Patrol published its national strategy in 2022 based on executive orders and national security guidance in lieu of a formal National Security Strategy or DHS Strategic Plan.

Appendix D:
Outdated CISA Critical Infrastructure Strategic Plans

Critical Infrastructure Plans	Purpose of the Critical Infrastructure and Sector-Specific Plans
National Plan (Last Published in 2013)	The National Plan guides the national effort to manage risk to the Nation's critical infrastructure from significant threat and hazards to physical and cyber critical infrastructure and requires an integrated approach across a diverse community. The success of this integrated approach depends on leveraging the full spectrum of capabilities, expertise, and experience across the critical infrastructure community and associated stakeholders.
Commercial Facilities Sector-Specific Plan (Last Published in 2015)	The Commercial Facilities Sector-Specific Plan describes how the commercial facilities sector manages risks, such as natural disasters, terrorist threats, cyberattacks, and geopolitical disruptions, and contributes to national critical infrastructure security and resilience.
Dams Sector-Specific Plan (Last Published in 2015)	The Dams Sector-Specific Plan sets the strategic direction for voluntary, collaborative efforts to improve security and resilience and tailors guidance to the operating conditions and risk landscape unique to the Dams Sector. The Dams Sector delivers critical water retention and control services in the United States. Therefore, complete or partial dam failure could result in sudden downstream flooding that causes casualties; major destruction and property damage; and cascading disruptions to the Electricity, Transportation Systems, Communications, and Water Sectors, among others.
Election Infrastructure Subsector-Specific Plan (Last Published in 2020)	The Election Infrastructure Subsector-Specific Plan outlines collaboration efforts and actions between public and private sector partners to protect election infrastructure and mitigate risk of hazards and threats, including natural disasters, terrorist attacks, cyberattacks, and other large-scale disruptions.
Energy Sector-Specific Plan (Last Published in 2015)	The Energy Sector-Specific Plan guides and integrates efforts to improve the security and resilience of critical infrastructure relevant to the Energy Sector. The Energy Sector, which PPD-21 identified as uniquely critical because it provides an essential function across virtually all critical infrastructure sectors, consists of widely diverse and geographically dispersed critical assets and systems that are often interdependent.

Critical Infrastructure Plans	Purpose of the Critical Infrastructure and Sector-Specific Plans
Government Facilities Sector-Specific Plan (Last Published in 2016)	The Government Facilities Sector-Specific Plan identifies and presents the unique characteristics and risk landscape of the Government Facilities Sector, which tightly integrates with other critical sector operations, creating interdependencies that could cause a disruption in one sector or impact to safe operations in another.
Communications Sector-Specific Plan (Last Published in 2015)	The Communications Sector-Specific Plan guides security and resilience efforts, informs partner decisions, and improves risk management practices for the Communications Sector. The Communications Sector is one of seven "community lifeline" services that enable the continuous operation of critical government and business functions and is essential to human health and safety and economic security. This sector depends on five other critical infrastructure sectors to ensure continued operation. Therefore, damage, disruption, or destruction to any one of these sectors could severely impact the operations of the Communications Sector.

Source: Obtained by DHS OIG from Critical Infrastructure and sector-specific plan documents

Appendix E:
Outdated FEMA National Planning Framework Guidance

Outdated National Planning Frameworks	Purpose of the National Planning Frameworks and Associated Annexes
Pandemic Crisis Action Plan (Last Published in 2018)	The Pandemic Crisis Action Plan operationalizes Biological Incident Annex to the Response and Recovery FIOPs with a focus on potential viral pandemic pathogens, outlines coordinated Federal response activities for a pandemic in the United States and clarifies roles and responsibilities of the Department of Health and Human Services, FEMA, Federal interagency partners, and other supporting agencies to establish lines of authority and to eliminate overlap and duplication of effort.
National Disaster Recovery Framework (Last Published in 2016)	The National Disaster Recovery Framework, part of the National Preparedness System, outlines the strategy and doctrine for how the whole community builds, sustains, and coordinates delivery of Recovery core capabilities identified in the National Preparedness Goal in an integrated manner with the other mission areas of Prevention, Protection, Mitigation, and Response.
Power Outage Incident Annex (Last Published in 2017)	The Power Outage Incident Annex provides the Federal Government's concept of operations and unified coordination structures required to execute survivor-centric response and recovery operations in the wake of a long-term power outage. Transportation, water, emergency services, healthcare, communications, and manufacturing represent only a few of the power grid's critical interdependencies. Therefore, reliance on the electric grid is a key interdependency (and vulnerability) among all critical infrastructure sectors and supporting infrastructures, making grid reliability and resilience a fundamental need for national safety and security.

Source: Obtained by DHS OIG from National Planning Framework Documents

Appendix F:
Major Contributors to This Report

Anthony Colache, Director
Michael Staver, Audit Manager
Rickey Smith, Auditor-in-Charge
Ashley Wilson, Auditor-in-Charge
Kenyon McGrone, Auditor
Victor Pena, Auditor
Kevin Dolloson, Communications Analyst
Nathaniel Nicholson, Referencer

Appendix G:
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Under Secretary, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information

To view this and any other DHS OIG reports, Please visit our website: www.oig.dhs.gov

For further information or questions, please contact the DHS OIG Office of Public Affairs via email: DHS-OIG.OfficePublicAffairs@oig.dhs.gov

DHS OIG Hotline

To report fraud, waste, abuse, or criminal misconduct involving U.S. Department of Homeland Security programs, personnel, and funds, please visit: www.oig.dhs.gov/hotline

If you cannot access our website, please contact the hotline by phone or mail:

Call: 1-800-323-8603

U.S. Mail:
Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive SW
Washington, DC 20528-0305