OFFICE OF INSPECTOR GENERAL

Independent Auditors' Report on the Department of Homeland Security's Consolidated Financial Statements for FYs 2022 and 2021 and Internal Control over Financial Reporting

Homeland Security

November 15, 2022

OIG-23-02

Washington, DC 20528 / www.oig.dhs.gov

November 15, 2022

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

FROM: Glenn Sklar GLENN E SKLAR Digitally signed by GLENN E SKLAR Date: 2022.11.15 12:39:06 -05'00'
Principal Deputy Inspector General

SUBJECT: *Independent Auditors' Report on the Department of Homeland Security's Consolidated Financial Statements for FYs 2022 and 2021 and Internal Control over Financial Reporting*

The attached report presents the results of an integrated audit of the Department of Homeland Security's consolidated financial statements for fiscal years 2022 and 2021 and internal control over financial reporting as of September 30, 2022. This audit is required by the *Chief Financial Officers Act of 1990,* as amended by the *Department of Homeland Security Financial Accountability Act* (October 16, 2004).

We contracted with the independent public accounting firm KPMG LLP (KPMG) to conduct the audit. The contract required that the audit be performed in accordance with U.S. generally accepted government auditing standards, Office of Management and Budget audit guidance, and the GAO/CIGIE *Financial Audit Manual.*

The Department achieved an unmodified (clean) opinion on all financial statements. However, KPMG issued an adverse opinion on DHS' internal control over financial reporting because of material weaknesses in internal control. KPMG identified material weaknesses in internal control in four areas and significant deficiencies in two areas. KPMG also reported two instances of noncompliance with laws and regulations.

Below are the areas in which KPMG identified material weaknesses and significant deficiencies, and laws and regulations with which KPMG identified noncompliance.

Material Weaknesses in Internal Control

- Information Technology Controls and Information Systems
- Financial Reporting
- Insurance Liabilities
- New System Obligations

Significant Deficiencies in Internal Control

- Custodial Activities: Seized and Forfeited Property
- Grants Management

Noncompliance with Laws and Regulations

- *Federal Managers' Financial Integrity Act of 1982* (FMFIA)
- *Federal Financial Management Improvement Act of 1996* (FFMIA)

Moving DHS' Financial Management Forward

This past fiscal year, the Department continued its commitment to identifying areas for improvement, developing and monitoring corrective actions, and establishing and maintaining effective internal control over financial reporting. Looking forward, to sustain a clean opinion on its financial statements and obtain a clean opinion on its internal control over financial reporting, the Department must continue remediation efforts and stay focused.

*****

KPMG is responsible for the attached Independent Auditors' Report dated November 14, 2022, and the conclusions expressed in the report. We do not express opinions on DHS' financial statements or internal control over financial reporting or conclusions on compliance and other matters.

Consistent with our responsibility under the *Inspector General Act of 1978, as amended*, 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 call me with any questions, or your staff may contact Bruce Miller, Deputy Inspector General for Audits, at (202) 981-6000.

Attachment

DHS OIG HIGHLIGHTS

Independent Auditors' Report on the Department of Homeland Security's Consolidated Financial Statements for FYs 2022 and 2021 and Internal Control over Financial Reporting

November 15, 2022

Why We Did This Audit

The *Chief Financial Officers Act of 1990* (Public Law 101-576) and the *Department of Homeland Security Financial Accountability Act* (Public Law 108-330) require us to conduct an annual audit of the Department of Homeland Security's consolidated financial statements and internal control over financial reporting.

What We Recommend

KPMG made 19 recommendations that, when implemented, may help improve the Department's internal control.

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

The independent public accounting firm KPMG LLP (KPMG) has issued an unmodified (clean) opinion on DHS' consolidated financial statements. KPMG noted that the financial statements present fairly, in all material respects, DHS' financial position as of September 30, 2022 and 2021.

KPMG issued an adverse opinion on DHS' internal control over financial reporting as of September 30, 2022. KPMG's report identified material weaknesses in internal control in four areas and other significant deficiencies in two areas. KPMG also reported instances of noncompliance with two laws and regulations.

Material Weaknesses

- Information Technology Controls and Information Systems
- Financial Reporting
- Insurance Liabilities
- New System Obligations

Other Significant Deficiencies

- Custodial Activities: Seized and Forfeited Property
- Grants Management

Noncompliance with Laws and Regulations

- Federal Managers' Financial Integrity Act of 1982
- Federal Financial Management Improvement Act of 1996

Management's Response

DHS concurred with all of the recommendations.

Table of Contents

Appendixes

KPMG LLP
Suite 12000
1801 K Street, NW
Washington, DC 20006

Independent Auditors' Report

Secretary and Inspector General
U.S. Department of Homeland Security:

Report on the Consolidated Financial Statements and Internal Control

Opinions on the Consolidated Financial Statements and Internal Control Over Financial Reporting

We have audited the consolidated financial statements of the U.S. Department of Homeland Security (DHS), which comprise the consolidated balance sheets as of September 30, 2022 and 2021, and the related consolidated statements of net costs, changes in net position, and custodial activity, and combined statements of budgetary resources for the years then ended, and the related notes to the consolidated financial statements. In our opinion, the accompanying consolidated financial statements present fairly, in all material respects, the financial position of DHS as of September 30, 2022 and 2021, and its net costs, changes in net position, budgetary resources, and custodial activity for the years then ended in accordance with U.S. generally accepted accounting principles.

We also have audited DHS's internal control over financial reporting as of September 30, 2022, based on criteria established in the *Standards for Internal Control in the Federal Government*, issued by the Comptroller General of the United States. In our opinion, because of the effect of the material weaknesses described in the Basis for Adverse Opinion on Internal Control Over Financial Reporting section on the achievement of the objectives of the control criteria, DHS has not maintained effective internal control over financial reporting as of September 30, 2022, based on criteria established in the *Standards for Internal Control in the Federal Government*, issued by the Comptroller General of the United States.

We considered the material weaknesses described in the Basis for Adverse Opinion on Internal Control Over Financial Reporting section in determining the nature, timing, and extent of audit procedures applied in our audit of the fiscal year 2022 consolidated financial statements, and the material weaknesses do not affect such report on the consolidated financial statements.

Basis for Opinions

We conducted our audits in accordance with auditing standards generally accepted in the United States of America (GAAS), the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States, and Office of Management and Budget (OMB) Bulletin No. 22-01, *Audit Requirements for Federal Financial Statements*. Our responsibilities under those standards and OMB Bulletin No. 22-01 are further described in the Auditors' Responsibilities for the Audit of the Consolidated Financial Statements section of our report. We are required to be independent of DHS and to meet our other ethical responsibilities, in accordance with the relevant ethical requirements relating to our audits. We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinions.

Basis for Adverse Opinion on Internal Control Over Financial Reporting

A material weakness is a deficiency, or a combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the entity's consolidated financial statements will not be prevented, or detected and corrected, on a timely basis. The following material weaknesses have been identified and included in the accompanying *Management's Report on Internal Control over Financial Reporting* and are further described in the accompanying Exhibits as items A through D.

A. Information Technology Controls and Information Systems
B. Financial Reporting
C. Insurance Liabilities
D. New System Obligations

Emphasis of Matter

As discussed in Note 15 to the consolidated financial statements, DHS had intragovernmental debt used to finance the National Flood Insurance Program (NFIP) of approximately $21 billion as of September 30, 2022 and 2021. The principal and interest payments are financed by the flood premiums from policyholders. Given the current rate structure, DHS will not be able to pay its debt from the premium revenue alone; therefore, DHS does not anticipate repaying the debt. Our opinion is not modified with respect to this matter.

Other Matters - Interactive Data

Management has elected to reference to information on websites or other forms of interactive data outside the *Agency Financial Report* to provide additional information for the users of its consolidated financial statements. Such information is not a required part of the consolidated financial statements or supplementary information required by the Federal Accounting Standards Advisory Board. The information on these websites or the other interactive data has not been subjected to any of our auditing procedures, and accordingly we do not express an opinion or provide any assurance on it.

Responsibilities of Management for the Consolidated Financial Statements and Internal Control Over Financial Reporting

Management is responsible for the preparation and fair presentation of the consolidated financial statements in accordance with U.S. generally accepted accounting principles, and for the design, implementation, and maintenance of effective internal control over financial reporting relevant to the preparation and fair presentation of consolidated financial statements that are free from material misstatement, whether due to fraud or error. Management is also responsible for its assessment about the effectiveness of internal control over financial reporting, included in the accompanying *Management's Report on Internal Control over Financial Reporting*.

Auditors' Responsibilities for the Audits of the Consolidated Financial Statements and Internal Control Over Financial Reporting

Our objectives are to obtain reasonable assurance about whether the consolidated financial statements as a whole are free from material misstatement, whether due to fraud or error, and about whether effective internal control over financial reporting was maintained in all material respects, and to issue an auditors' report that includes our opinions.

Reasonable assurance is a high level of assurance but is not absolute assurance and therefore is not a guarantee that an audit of consolidated financial statements or an audit of internal control over financial reporting conducted in accordance with GAAS, *Government Auditing Standards,* and OMB Bulletin No. 22-01 will always detect a material misstatement or a material weakness when it exists. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control. Misstatements are considered to be material if there is a substantial likelihood that, individually or in the aggregate, they would influence the judgment made by a reasonable user based on the consolidated financial statements.

In performing an audit of consolidated financial statements and an audit of internal control over financial reporting in accordance with GAAS, *Government Auditing Standards,* and OMB Bulletin No. 22-01, we:

- Exercise professional judgment and maintain professional skepticism throughout the audits.

- Identify and assess the risks of material misstatement of the consolidated financial statements, whether due to fraud or error, and design and perform audit procedures responsive to those risks. Such procedures include examining, on a test basis, evidence regarding the amounts and disclosures in the consolidated financial statements.
- Obtain an understanding of internal control relevant to the consolidated financial statement audit in order to design audit procedures that are appropriate in the circumstances.
- Obtain an understanding of internal control over financial reporting relevant to the audit of internal control over financial reporting, assess the risks that a material weakness exists, and test and evaluate the design and operating effectiveness of internal control over financial reporting based on the assessed risk.
- Evaluate the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluate the overall presentation of the consolidated financial statements.

We are required to communicate with those charged with governance regarding, among other matters, the planned scope and timing of the audit, significant audit findings, and certain internal control related matters that we identified during the consolidated financial statement audit.

We did not test all internal controls relevant to operating objectives as broadly defined by the *Federal Managers' Financial Integrity Act of 1982.*

Definition and Inherent Limitations of Internal Control Over Financial Reporting

An entity's internal control over financial reporting is a process effected by those charged with governance, management, and other personnel, designed to provide reasonable assurance regarding the preparation of reliable financial statements in accordance with U.S. generally accepted accounting principles. An entity's internal control over financial reporting includes those policies and procedures that (1) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the entity; (2) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with U.S. generally accepted accounting principles, and that receipts and expenditures of the entity are being made only in accordance with authorizations of management and those charged with governance; and (3) provide reasonable assurance regarding prevention, or timely detection and correction of unauthorized acquisition, use, or disposition of the entity's assets that could have a material effect on the financial statements.

Because of its inherent limitations, internal control over financial reporting may not prevent, or detect and correct, misstatements. Also, projections of any assessment of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

Required Supplementary Information

U.S. generally accepted accounting principles require that the information in the Management's Discussion and Analysis and Required Supplementary Information sections be presented to supplement the basic consolidated financial statements. Such information is the responsibility of management and, although not a part of the basic consolidated financial statements, is required by the Federal Accounting Standards Advisory Board, who considers it to be an essential part of financial reporting for placing the basic consolidated financial statements in an appropriate operational, economic, or historical context. We have applied certain limited procedures to the required supplementary information in accordance with GAAS, which consisted of inquiries of management about the methods of preparing the information and comparing the information for consistency with management's responses to our inquiries, the basic consolidated financial statements, and other knowledge we obtained during our audits of the basic consolidated financial statements. We do not express an opinion or provide any assurance on the information because the limited procedures do not provide us with sufficient evidence to express an opinion or provide any assurance.

Other Information

Management is responsible for the other information included in the *Agency Financial Report*. The other information comprises the About this Report, Message from the Secretary, Message from the Chief Financial Officer, Introduction, Other Information, and Acronym List sections but does not include the consolidated financial statements and our auditors' report thereon. Our opinion on the consolidated financial statements does not cover the other information, and we do not express an opinion or any form of assurance thereon.

In connection with our audit of the consolidated financial statements, our responsibility is to read the other information and consider whether a material inconsistency exists between the other information and the consolidated financial statements, or the other information otherwise appears to be materially misstated. If, based on the work performed, we conclude that an uncorrected material misstatement of the other information exists, we are required to describe it in our report.

Other Reporting on Internal Control

In accordance with *Government Auditing Standards*, we are required to report findings of significant deficiencies. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. We consider the deficiencies described in the accompanying Exhibits as items E and F to be significant deficiencies.

E. Custodial Activities: Seized and Forfeited Property
F. Grants Management

Report on Compliance and Other Matters

As part of obtaining reasonable assurance about whether DHS's consolidated financial statements as of and for the year ended September 30, 2022 are free from material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the consolidated financial statements. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests disclosed instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards* or OMB Bulletin No. 22-01, and which are described in the accompanying Exhibits as item G.

G. *Federal Managers' Financial Integrity Act of 1982* (FMFIA)

We also performed tests of DHS's compliance with certain provisions referred to in Section 803(a) of the *Federal Financial Management Improvement Act of 1996* (FFMIA). Providing an opinion on compliance with FFMIA was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests disclosed instances, described in the accompanying Exhibits, in which DHS's financial management systems did not substantially comply with the Federal financial management systems requirements, applicable Federal accounting standards, or application of the United States Government Standard General Ledger at the transaction level.

DHS's Response to Findings

Government Auditing Standards requires the auditor to perform limited procedures on DHS's response to the findings identified in our audit and described in Appendix A. DHS's response was not subjected to the other auditing procedures applied in the audit of the consolidated financial statements or the audit of internal control over financial reporting and, accordingly, we express no opinion on the response.

Purpose of the Reporting Required by Government Auditing Standards

The purpose of the communication described in the Other Reporting on Internal Control and the Report on Compliance and Other Matters sections is solely to describe the deficiencies we consider to be significant deficiencies and the scope of our testing of compliance and the results of that testing, and not to provide an opinion on compliance. Accordingly, this communication is not suitable for any other purpose.

KPMG LLP

Washington, D.C.
November 14, 2022

The weaknesses in internal control over financial reporting (internal control) existed as of September 30, 2022, and the instances of noncompliance with certain provisions of laws, regulations, contracts, and grant agreements were identified during the year ended September 30, 2022. The determination of which control deficiencies rise to the level of a material weakness or a significant deficiency is based on an evaluation of the impact of control deficiencies identified in all components, considered individually and in the aggregate, on the DHS consolidated financial statements as of September 30, 2022. Component-level deficiencies vary in severity. The associated entity level controls, as defined by the Government Accountability Office's *Standards for Internal Control in the Federal Government,* issued by the Comptroller General of the United States (Green Book), are also identified in relation to the control activities in the corresponding areas of the following Exhibits.

The findings are presented in three Exhibits:

Exhibit I Material Weaknesses. A material weakness is a deficiency, or combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. DHS has material weaknesses within each of the following areas:

A. Information Technology Controls and Information Systems
B. Financial Reporting
C. Insurance Liabilities
D. New System Obligations

Exhibit II Significant Deficiencies. A significant deficiency is a deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by DHS management and others in positions of DHS oversight. DHS has significant deficiencies within each of the following areas:

E. Custodial Activities: Seized and Forfeited Property
F. Grants Management

Exhibit III Compliance and Other Matters. The compliance and other matters identified included instances of noncompliance with certain provisions of laws, regulations, contracts, and grant agreements, and other matters that are required to be reported under *Government Auditing Standards* or Office of Management and Budget (OMB) Bulletin No. 22-01, *Audit Requirements for Federal Financial Statements*. DHS has instances of noncompliance as follows:

G. *Federal Managers' Financial Integrity Act of 1982*
H. *Federal Financial Management Improvement Act of 1996*

Criteria DHS's internal control over financial reporting is based on the criteria established by the Green Book.

I-A Information Technology Controls and Information Systems

Background:

Information technology (IT) controls are a critical subset of an entity's internal control. There are two main types of IT controls: IT general controls (ITGCs) and application controls. ITGCs operate over entire or large portions of systems and represent the foundation of an IT control structure. They are applied at the entity-wide, operating system, database, or application level, and include controls over access, segregation of duties, configuration management, and security management. Effective ITGCs are necessary to create the foundation for the operation of application controls. Application controls are those controls that directly relate to specific IT applications and ensure completeness, accuracy, validity, confidentiality, and availability of data. The deficiencies indicated in this Exhibit are representative of ITGC and application control deficiencies at headquarters and various components across DHS including U.S. Customs and Border Protection (CBP), Federal Emergency Management Agency (FEMA), U.S. Immigration and Customs Enforcement (ICE), Transportation Security Administration (TSA), U.S. Coast Guard (USCG), and U.S. Citizenship and Immigration Services (USCIS).

Conditions:

DHS did not design and implement the entity's information systems and related control activities to achieve objectives and respond to risks as required by Green Book principles 11, *Design Activities for the Information System*, and 12, *Implement Control Activities*. Specifically, DHS had:

- Ineffective design, implementation, or operating effectiveness of ITGCs over IT operating systems, databases, and applications supporting financial reporting processes across DHS in the following areas:

  Access control and segregation of duties

  - User, service, shared, privileged, and generic (including emergency, temporary, developer, and migrator) accounts not properly authorized, recertified, and revoked timely;
  - The principles of least privilege and segregation of duties not applied;
  - Login events not monitored or reviewed;

  Configuration management

  - Systems not properly configured;
  - System changes not documented, authorized, or monitored;

  Security management

  - Assessments and documentation required for a system Authority to Operate (ATO) not completed or approved;
  - Internal manuals not timely updated for current industry guidance; and
  - Identified vulnerabilities not timely remediated.
- Ineffective implementation of ITGCs prior to system migration.
- Ineffective design, implementation, or operating effectiveness of ITGCs at service organizations.
- Ineffective operating effectiveness of application controls and manual controls that are dependent upon the information derived from DHS information systems.

DHS continued to have deficiencies in its design and implementation of controls related to information technology. These deficiencies have persisted since the inception of DHS. As a result, DHS did not remediate identified internal control deficiencies on a timely basis as required by Green Book principle 17, *Evaluate Issues and Remediate Deficiencies*. Specifically, DHS had:

- Ineffective design and implementation of controls to remediate IT findings, including insufficient corrective actions to address deficiencies that have existed for several years in multiple information systems.

Causes:

These deficiencies are a result of the failure of entity level controls, as follows:

Green Book principle 7 requires that "Management should identify, analyze, and respond to risks related to achieving the defined objectives." DHS did not effectively implement and operate Green Book principle 7. Specifically:

- DHS did not fully implement a robust risk assessment to identify and mitigate the risks arising from IT.
- DHS did not resolve the risks created by historic limitations in the functionality of its information systems.
- DHS did not successfully mitigate the risk created by implementing manual controls to compensate for risks resulting from decentralized systems and records management processes or utilities with limited automated capabilities.

Green Book principle 14 requires that "Management should internally communicate the necessary quality information to achieve the entity's objectives." DHS did not effectively implement and operate Green Book principle 14. Specifically:

- DHS did not communicate internally to properly authorize, recertify, or revoke access to systems or to authorize and monitor system changes.
- DHS did not timely update and distribute internal manuals based on industry guidance.

Green Book principle 16 requires that "Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results." DHS did not effectively implement and operate Green Book principle 16. Specifically:

- DHS did not effectively implement a formalized process to monitor the third-party service organizations responsible for maintaining the infrastructure support for various IT systems.
- DHS established corrective action plans but did not effectively monitor them to track progress towards timely remediation of deficiencies.

Effects:

Deficiencies in access controls and segregation of duties increase the risk that current employees, separated employees, or contractors may obtain unauthorized or inappropriate access to information systems or data. Such access could lead to unauthorized activities or inappropriate disclosures of sensitive data. Deficiencies in configuration management increase the risk that unauthorized or inappropriate changes to systems will be applied and go undetected by management, resulting in lower assurance that information systems will operate as intended and that data is reliable, valid, and complete. Deficiencies in security management increase the risk that system vulnerabilities will not be identified and remediated, compromising the reliability and integrity of data and increasing the risk of data loss.

In addition, system limitations contribute to deficiencies in multiple financial process areas across DHS. Many key DHS information systems are not compliant with Federal financial management system requirements as defined by FFMIA, as noted in Exhibit III. These system limitations cause a greater risk of error and result in inconsistent, incomplete, or inaccurate control execution.

Collectively, DHS's lack of an appropriate risk assessment to identify and mitigate the ITGC and application control deficiencies limits DHS's ability to process, store, and report financial data in a manner that ensures accuracy, confidentiality, integrity, and availability. In some cases, in response to these deficiencies, DHS intended to utilize manual controls; however, these manual controls often were not properly designed or implemented, or did not operate effectively, as reported in Exhibits I and II.

Recommendations:

We recommend that DHS:

1. Office of the Chief Financial Officer (OCFO), in coordination with the Office of the Chief Information Officer (OCIO), the Office of the Chief Information Security Officer (OCISO), and component IT and financial management, complete a comprehensive risk analysis and develop a mitigation plan to reduce risks related to ITGC and application control deficiencies timely;

2. OCFO, in coordination with the OCIO, the OCISO, and component IT and financial management, design, implement, and communicate effective internal control processes to address the risk of errors due to IT system functionality issues, the inability to rely on information derived from systems, and the inability to rely on application controls until system deficiencies are remediated;

3. OCISO, the OCIO, and component IT management sufficiently monitor IT vulnerabilities and limitations, and coordinate with the OCFO and component financial management to implement manual controls to mitigate risk;

4. OCFO, in coordination with the OCIO, the OCISO, and component IT and financial management, design and implement an effective internal control process to review service organization risks and evaluate ineffective service organization ITGCs and design and implement appropriate compensating controls; and

5. OCFO, in coordination with the OCIO, the OCISO, and component IT and financial management, develop, implement, and monitor internal manuals and corrective action plans.

I-B Financial Reporting

Background:

Internal control is a process effected by those charged with governance, management, and other personnel, and is designed to provide reasonable assurance regarding the preparation of reliable financial statements in accordance with U.S. generally accepted accounting principles.

Conditions:

DHS did not design control activities to achieve internal control objectives and respond to risks as required by Green Book principle 10, *Design Control Activities*, or implement the entity's information systems and related control activities through policies as required by Green Book principles 11, *Design Activities for the Information System*, and 12, *Implement Control Activities*. Specifically, DHS had:

- Ineffective design, implementation, or operating effectiveness of controls supporting financial reporting processes across DHS in the following areas:

  Journal entries

  - Recurring manual journal entries not analyzed for completeness at USCG;
  - Manual journal entry amounts and attributes not validated with appropriate supporting documentation at CBP and USCG;

  Service organization control (SOC) reports

  - Service provider risks not addressed by obtaining and effectively reviewing SOC reports, or by assessing the risks when a SOC report does not exist, at multiple components across DHS;

  Application controls and information derived from systems

  - Manual controls to compensate for application control deficiencies not designed and implemented at multiple components across DHS;
  - Baseline assessments of application controls and information derived from systems with effective ITGCs not performed at CBP and ICE;

  Application of accounting standards

  - Accounting standards related to the recognition and disclosure of certain liabilities not properly reviewed at FEMA; and

  Response to risk presented by the USCG financial system migration

  - Risks over various business processes not adequately identified, analyzed, or responded to at USCG.

DHS continued to have deficiencies in its design and implementation of controls over Financial Reporting. DHS did not remediate identified internal control deficiencies on a timely basis as required by Green Book principle 17, *Evaluate Issues and Remediate Deficiencies*.

Causes:

These deficiencies are a result of the failure of entity level controls as follows:

Green Book principle 5 requires that "Management should evaluate performance and hold individuals accountable for their internal control responsibilities." DHS did not effectively implement and operate Green Book principle 5. Specifically:

- DHS did not enforce accountability of personnel responsible for the review of SOC reports.

Green Book principle 7 requires that "Management should identify, analyze, and respond to risks related to achieving the defined objectives." DHS did not effectively implement and operate Green Book principle 7. Specifically:

- DHS did not sufficiently respond to the risk posed by incomplete or inaccurate journal entry supporting documentation.
- DHS did not fully implement a robust risk assessment to identify and mitigate the risks arising from IT, including those related to inappropriate reliance on information derived from systems.
- DHS did not assess the risks created by IT deficiencies and their impact on other controls.

Green Book principle 9 requires that "Management should identify, analyze, and respond to significant changes that could impact the internal control system." DHS did not effectively implement and operate Green Book principle 9. Specifically:

- DHS did not sufficiently identify, analyze, and respond to the changes presented by USCG's financial system migration and certain programs at FEMA.

Green Book principle 13 requires that "Management should use quality information to achieve the entity's objectives." DHS did not effectively implement and operate Green Book principle 13. Specifically:

- DHS did not obtain the appropriate information timely to support proposed journal entries.
- DHS did not process data into quality information that was useable for operating controls effectively.
- DHS did not perform baseline testing of information generated by applications prior to relying on that information as part of a control.

Green Book principle 16 requires that "Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results." DHS did not effectively implement and operate Green Book principle 16. Specifically:

- DHS did not perform continuous monitoring and testing of IT and financial controls for all significant areas, including monitoring the activities and controls performed by service organizations.
- DHS did not sufficiently monitor the status of corrective action plans.
- DHS did not design and implement sufficient procedures to review SOC reports, including identification and assessment of complementary user entity controls.
- DHS did not monitor changes to the internal control system to identify the need for a liability disclosure.

Effects:

The failure to adequately design, implement, and operate internal controls over journal entries resulted in misstatements that occurred without being prevented, or detected and corrected timely.

The failure to adequately design, implement, and operate internal controls related to oversight of service organizations increases the risk that misstatements can occur without being prevented, or detected and corrected timely.

The failure to adequately identify, analyze, and assess changes to the internal control system, including the risks arising from the implementation of a new financial system, increases the risk that the financial information used in controls is not reliable. This failure also resulted in the omission of a liability disclosure, which management subsequently corrected.

The failure to adequately design, implement, and operate internal controls related to the baseline assessment of application controls and information derived from systems prevents management from relying on application controls. It also prevents management from relying on the information derived from systems used to record transactions and perform control activities.

The lack of compensating controls for IT deficiencies also results in noncompliance with Federal financial management system requirements, as defined by FFMIA and reported in Exhibit III.

The improper review of accounting standards also results in noncompliance with FFMIA, as reported in Exhibit III.

The failure to perform continuous monitoring and testing of IT and financial controls results in lack of timely remediation of existing deficiencies and noncompliance with FMFIA, as reported in Exhibit III.

Recommendations:

We recommend that DHS:

6. perform an analysis to assess the risks of the migration to a new general ledger system and implement controls to ensure all necessary journal entries are completely recorded each period;
7. develop new policies or improve and reinforce existing policies, procedures, and related internal controls, to ensure journal entries are adequately researched, supported, and reviewed before and after recording in the general ledger;
8. enforce accountability for adherence to policies and procedures and provide the necessary financial reporting oversight;
9. improve the process for identification, analysis, and response over significant changes and updates to risks assessments related to financial reporting, including risks associated with changes to financial systems and new liabilities;
10. align knowledgeable individuals to monitor and evaluate the roles of service organizations, assess controls at those service organizations, and identify and assess complementary user entity controls within the components relying on those service organizations; and
11. improve monitoring controls over assessing internal controls and remediating known internal control deficiencies timely.

I-C Insurance Liabilities

Background:

DHS manages the NFIP, a program to provide flood insurance to policyholders through a network of write-your-own (WYO) insurance companies. These insurance companies provide services on behalf of DHS, including underwriting premium policies and processing claims. DHS used the WYO data, along with NFIP loss and loss adjustment expense factors, to estimate the liabilities. DHS's insurance liabilities include an actuarially derived insurance liability for claims incurred but not yet reported and a liability for losses on remaining coverage as of September 30, 2022. The liability for losses on remaining coverage results from DHS's FY 2022 implementation of a new premium policy rating system referred to as Risk Rating 2.0.

Conditions:

DHS did not design control activities to achieve objectives and respond to risks as required by Green Book principle 10, *Design Control Activities*, or implement the related control activities through policies as required by Green Book principle 12, *Implement Control Activities*. Specifically, at FEMA, DHS had:

- Insufficient design of the controls over the validation of the underlying data used in the valuation of the flood insurance liabilities; and
- Insufficient design and implementation of the controls over the assumptions, methods, and models used in the valuation of the flood insurance liabilities.

Causes:

These deficiencies are a result of the failure of entity level controls as follows:

Green Book principle 3 requires that "Management develops and maintains documentation of its internal control system." DHS did not effectively implement and operate Green Book principle 3. Specifically:

- DHS did not adequately document the determination and appropriateness of the methods, models, and assumptions used in the actuarial insurance liability estimates.

Green Book principle 5 requires that "Management should evaluate performance and hold individuals accountable for their internal control responsibilities." DHS did not effectively implement and operate Green Book principle 5. Specifically:

- DHS did not enforce accountability of personnel responsible for reviewing the underlying data and the appropriateness of the assumptions, methods, and models used in the actuarial insurance liability estimates.

Green Book principle 9 requires that "Management should identify, analyze, and respond to significant changes that could impact the internal control system." DHS did not effectively implement and operate Green Book principle 9. Specifically:

- DHS did not properly assess and document the appropriateness of changes to the methods, models, and assumptions for the actuarial insurance liability estimates.

DHS continued to have deficiencies in its design and implementation of controls over insurance liabilities. DHS did not remediate identified internal control deficiencies on a timely basis as required by Green Book principle 17, *Evaluate Issues and Remediate Deficiencies*.

Effect:

The failure to adequately design, implement, and operate internal controls over the actuarially derived estimates increases the risk that misstatements to insurance liabilities on the Balance Sheet can occur without being prevented, or detected and corrected, timely.

Recommendations:

We recommend that DHS:

12. develop new policies, or improve and reinforce existing policies, procedures, and related internal controls, to ensure that:
    a. the underlying data to actuarially derived estimates is reviewed timely;
    b. information derived from the systems used in the operations of controls is determined to be complete and accurate;
    c. risks related to the methods, models, assumptions, and data elements are assessed each year to identify, plan, and respond to changes; and
    d. changes to the methods, models, assumptions, and data elements are sufficiently documented.

I-D New System Obligations

Background:

In FY 2022, USCG migrated to a new financial system. The financial system migration resulted in significant changes to existing processes, including changes to the process for recording obligations and expenditures incurred against obligations. USCG personnel record key data elements for new contracts and receipts of goods and services in the financial system, which drive the accounting for the transactions.

Conditions:

DHS did not design control activities to achieve objectives and respond to risks as required by Green Book principle 10, *Design Control Activities*, or implement the related control activities through policies as required by Green Book principle 12, *Implement Control Activities*. Specifically, at USCG, DHS had:

- Insufficient design and implementation of controls over the review of obligations incurred; and
- Insufficient design and implementation of controls over recording the receipt of goods and services to ensure the accuracy of expenditure records.

Causes:

These deficiencies are a result of the failure of entity level controls as follows:

Green Book principle 3 requires that "Management develops and maintains documentation of its internal control system." DHS did not effectively implement and operate Green Book principle 3. Specifically:

- DHS did not adequately document changes to their internal control system to allow control owners to effectively operate controls over obligations incurred and the related expenditures.

Green Book principle 4 requires that "Management recruits, develops, and retains competent personnel to achieve the entity's objectives." DHS did not effectively implement and operate Green Book principle 4. Specifically:

- DHS did not sufficiently train control owners on the necessary knowledge and skills related to the new financial system to enable them to properly operate controls over obligations incurred and the related expenditures.

Green Book principle 7 requires that "Management should identify, analyze, and respond to risks related to achieving the defined objectives." DHS did not effectively implement and operate Green Book principle 7. Specifically:

- DHS did not fully implement a robust risk assessment to identify and mitigate the risks arising from IT.
- DHS did not assess the risks created by IT deficiencies and their impact on other controls.

Green Book principle 9 requires that "Management should identify, analyze, and respond to significant changes that could impact the internal control system." DHS did not effectively implement and operate Green Book principle 9. Specifically:

- DHS did not sufficiently identify, analyze, and respond to the risks presented by USCG's financial system migration.

Effects:

The failure to adequately design, implement, and operate internal controls over the review of obligations incurred and related expenditures increases the risk that misstatements to obligations incurred and upward adjustments on the Statement of Budgetary Resources and expenditures on the Balance Sheet and Statement of Net Cost can occur without being prevented, or detected and corrected, timely. These deficiencies resulted in misstatements to Other Liabilities and Accounts Payable on the Balance Sheet.

Recommendations:

We recommend that DHS:

13. perform a robust risk assessment related to the financial system migration and design and implement controls to respond to identified risks; and
14. provide training to enable control operators to properly perform control responsibilities.

II-E Custodial Activities: Seized and Forfeited Property

Background:

DHS is responsible for reporting seized and forfeited property that is in its custody. DHS seizes various items, including prohibited drugs and counterfeit goods. DHS relies on several of its components to enter case information, including weights and measures, into the seized and forfeited property system.

Conditions:

DHS did not design and implement control activities to achieve objectives and respond to risks as required by Green Book principle 10, *Design Control Activities*, or implement control activities through policies as required by Green Book principle 12, *Implement Control Activities*. Specifically, at CBP and ICE, DHS had:

- Ineffective design, implementation, and operating effectiveness of controls over seized and forfeited asset transactions not recorded properly and timely in the seized and forfeited assets tracking system by CBP and ICE personnel.

Causes:

These deficiencies are a result of the failure of entity level controls as follows:

Green Book principle 7 requires that "Management should identify, analyze, and respond to risks related to achieving the defined objectives." DHS did not effectively implement and operate Green Book principle 7. Specifically:

- DHS did not respond to identified risks related to seized and forfeited property information inputted and updated in the system of record.

Green Book principle 13 requires that "Management should use quality information to achieve the entity's objectives." DHS did not effectively implement and operate Green Book principle 13. Specifically:

- DHS did not use reliable information to identify the need to revise seized and forfeited property information, when necessary.

DHS continued to have deficiencies in its design and implementation of controls over seized and forfeited property. DHS did not remediate identified internal control deficiencies on a timely basis as required by Green Book principle 17, *Evaluate Issues and Remediate Deficiencies*.

Effect:

Failure to effectively operate control activities related to seized and forfeited property resulted in misstatements of the Seized and Forfeited Property note to the financial statements.

Recommendation:

We recommend that DHS:

15. enhance existing controls, including using quality information, to prevent and detect material errors in the seized property footnote.

II-F Grants Management

Background:

DHS manages multiple Federal disaster and non-disaster grant programs, as well as other needs assistance programs, including programs related to the coronavirus pandemic. In FY 2018, DHS began implementation of the process to standardize all grant management activities, which continued into FY 2022. This included coordination among the grant regional offices and central management as well as among the various grant programs. To monitor the spending of the disaster and non-disaster grant funding, DHS performs site visits and monitors Federal Financial Reports submitted by grant recipients.

Conditions:

DHS did not design control activities to achieve objectives and respond to risks as required by Green Book principle 10, *Design Control Activities*, or implement control activities through policies as required by Green Book principle 12, *Implement Control Activities.* Specifically, at FEMA, DHS had:

- Ineffective controls over monitoring of grant recipients; and
- Insufficient delegation of authority documentation for controls over the review of disaster grant obligations and deobligations.

Causes:

These deficiencies are a result of the failure of entity level controls as follows:

Green Book principle 5 requires that "Management should evaluate performance and hold individuals accountable for their internal control responsibilities." DHS did not effectively implement and operate Green Book principle 5. Specifically:

- DHS did not enforce accountability of personnel responsible for monitoring grant recipients and documenting the delegation of authority for the review of disaster grant obligations and deobligations.

Green Book principle 7 requires that "Management should identify, analyze, and respond to risks related to achieving the defined objectives." DHS did not effectively implement and operate Green Book principle 7. Specifically:

- DHS did not establish control thresholds to determine the appropriate scope of grant monitoring site visits and desk reviews to minimize residual risk.

DHS continued to have deficiencies in its design and implementation of controls over grants management. DHS did not remediate identified internal control deficiencies on a timely basis as required by Green Book principle 17, *Evaluate Issues and Remediate Deficiencies*.

Effects:

The failure to enforce the accountability of personnel during FY 2022 caused ineffective monitoring of open and closed grants. Ineffective monitoring may result in inaccurate or unauthorized expense reporting by grant recipients and increases the risk that DHS may not identify corrective actions for grant recipients timely. Unauthorized approval of disaster grant obligations and deobligations increases the risk that misstatements can occur without being prevented, or detected and corrected, timely.

Recommendations:

We recommend that DHS:

16. perform a robust risk assessment to assess and minimize the residual risk related to unmonitored grants; and
17. enforce accountability for adherence to policies and procedures for monitoring grant recipients and documenting the delegation of authority for the review of disaster grant obligations and deobligations.

III-G ***Federal Managers' Financial Integrity Act of 1982***

FMFIA requires agencies to establish effective internal control and information systems, and to continuously evaluate and assess the effectiveness of their internal control. DHS has implemented a multi-year plan to implement OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, to comply with FMFIA. However, the DHS *Secretary's Assurance Statement*, dated November 14, 2022, as presented in *Management's Discussion and Analysis* of DHS's FY 2022 *Agency Financial Report*, acknowledged the existence of control activities demonstrating material weaknesses, and therefore provided qualified assurance that internal control over financial reporting was operating effectively as of September 30, 2022. Management's findings were similar to the control deficiencies described in Exhibits I and II. DHS did not perform continuous monitoring and testing of both IT and financial controls for all significant areas.

In FY 2022, DHS did not fully establish effective systems, processes, policies, and testing procedures to ensure that internal controls were operating effectively throughout DHS. Deficiencies related to monitoring the internal control system are discussed in Exhibit I, Sections **I-A**, *Information Technology Controls and Information Systems*, and **I-B**, *Financial Reporting*.

Recommendation:

We recommend that DHS:

18. continue its corrective actions to address internal control deficiencies to ensure compliance with FMFIA, and implement the recommendations provided in Exhibits I and II.

III-H *Federal Financial Management Improvement Act of 1996*

FFMIA Section 803(a) requires that agency Federal financial management systems comply with: (1) applicable Federal accounting standards; (2) Federal financial management system requirements; and (3) the USSGL at the transaction level. FFMIA emphasizes the need for agencies to have systems that can generate timely, reliable, and useful information with which to make informed decisions to ensure ongoing accountability.

As of September 30, 2022, DHS did not comply with applicable Federal accounting standards, Federal financial management system requirements, and application of the USSGL at the transaction level, as described in Exhibit I, Section **I-A**, *Information Technology Controls and Information Systems*, Exhibit I, Section **I-B**, *Financial Reporting*, and Exhibit I, Section **I-C**, *New System Obligations*. The DHS Secretary stated in the *Secretary's Assurance Statement,* dated November 14, 2022, that DHS's financial management systems did not substantially comply with government-wide requirements mandated by FFMIA. DHS's remedial actions and related timeframes are also presented in Table 3 of *Management's Discussion and Analysis* in the FY 2022 *Agency Financial Report*.

Recommendation:

We recommend that DHS:

19. improve its financial management systems to ensure compliance with FFMIA, and implement the recommendations provided in Exhibit I.

Appendix A
Management Comments to the Draft Report

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

Homeland Security

November 14, 2022

MEMORANDUM FOR: The Honorable Joseph V. Cuffari
Inspector General

FROM: Stacy Marcott
Senior Official Performing the Duties of the Chief Financial Officer

STACY A MARCOTT

Digitally signed by STACY A MARCOTT
Date: 2022.11.10 15:36:19 -05'00'

SUBJECT: Fiscal Year 2022 Financial Statement and Internal Control Over Financial Reporting Audit

Thank you for your audit report on the Department's Financial Statements and Internal Control over Financial Reporting for Fiscal Years (FY) 2022 and 2021. We agree with the Independent Public Accountant's conclusion. We are pleased to have earned an unmodified (clean) opinion on our consolidated financial statements for the tenth consecutive year.

The Department continues to prioritize maturing information technology controls and is implementing an aggressive plan to modernize our financial systems. In early FY 2022, the United States Coast Guard (USCG) migrated to our new Financial Systems Modernization Solution (FSMS). Migrating a complex system to a new platform presented challenges we worked to overcome throughout the year. Our focus for FY 2023 is to apply these lessons learned and opportunities to refine USCG financial system performance, accounting, and reporting.

The Department is committed to advancing our controls and remediating known challenges using a multi-year, risk-based approach.

I look forward to our continued partnership and collaboration with the Office of the Inspector General and the Independent Public Accountant in the years ahead.

Appendix B
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
DHS Chief Information Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information and Copies

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.
Follow us on Twitter at: @dhsoig.

OIG Hotline

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

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