OFFICE OF INSPECTOR GENERAL

Independent Auditors' Report on DHS' FY 2017 Financial Statements and Internal Control over Financial Reporting

Homeland Security

November 15, 2017

OIG-18-16

DHS OIG HIGHLIGHTS

Independent Auditors' Report on DHS' FY 2017 Financial Statements and Internal Control over Financial Reporting

November 15, 2017

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 (DHS) consolidated financial statements and internal control over financial reporting.

What We Recommend

KPMG LLP made 56 recommendations that, when implemented, would help improve the Department's internal control.

For Further Information:
Contact our Office of Public Affairs at (202) 254-4100, 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, 2017.

KPMG issued an adverse opinion on DHS' internal control over financial reporting as of September 30, 2017. The report identifies the following six significant deficiencies in internal control, the first two of which are considered material weaknesses, and four instances where DHS did not comply with four laws and regulations:

Significant Deficiencies

1. Information Technology Controls and Financial System Functionality
2. Financial Reporting
3. Entity-Level Controls
4. Property, Plant, and Equipment
5. Custodial Activities
6. Grants Management

Laws and Regulations with Instances of Noncompliance

1. Federal Managers' Financial Integrity Act of 1982
2. Single Audit Act Amendments of 1996
3. Anti-deficiency Act
4. Federal Financial Management Improvement Act of 1996

Management's Response

The Department concurred with the independent auditors' conclusion and indicated that management will continue to implement corrective action to improve financial management and internal control.

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

NOV 15 2017

MEMORANDUM FOR: The Honorable Elaine C. Duke
Acting Secretary
Department of Homeland Security

FROM: John Roth
Inspector General

SUBJECT: *Independent Auditors' Report on DHS' FY 2017 Financial Statements and Internal Control over Financial Reporting*

The attached report presents the results of an integrated audit of the Department of Homeland Security's (DHS) fiscal year (FY) 2017 financial statements and internal control over financial reporting. This is a mandatory audit required by the *Chief Financial Officers Act of 1990,* as amended by the *Department of Homeland Security Financial Accountability Act of 2004*. This report is incorporated into the Department's FY 2017 *Agency Financial Report*. We contracted with the independent public accounting firm KPMG LLP (KPMG) to conduct the audit.

The Department continued to improve financial management in FY 2017 and 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.

Summary

KPMG identified six significant deficiencies in internal control, of which two are considered material weaknesses. DHS also identified the same material weaknesses in the *Secretary's Assurance Statement*.

The following are the two significant deficiencies in internal control considered to be material weaknesses, the four other significant deficiencies in internal control, and the four laws and regulations with which KPMG identified instances of DHS' noncompliance:

Significant Deficiencies Considered To Be Material Weaknesses

- Information Technology Controls and Financial System Functionality
- Financial Reporting

Other Significant Deficiencies

- Entity-Level Controls
- Property, Plant, and Equipment
- Custodial Activities: Entry Process and Refunds and Drawback
- Grants Management

Laws and Regulations with Identified Instances of Noncompliance

- *Federal Managers' Financial Integrity Act of 1982*
- *Single Audit Act Amendments of 1996*
- *Anti-deficiency Act*
- *Federal Financial Management Improvement Act of 1996*

Moving DHS' Financial Management Forward

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

*****

KPMG is responsible for the attached Independent Auditors' Report dated November 14, 2017, and the conclusions expressed in the report. To ensure the quality of the audit work performed, we evaluated KPMG's qualifications and independence, reviewed the approach and planning of the audit, monitored the progress of the audit at key points, reviewed and accepted KPMG's audit report, and performed other procedures that we deemed necessary. Additionally, we provided oversight of the audit of financial statements and certain accounts and activities conducted at key components within the Department. Our review, as differentiated from an audit in accordance with generally accepted government auditing standards, was not intended to enable us to express, and we do not express, an opinion on the financial statements or internal control or provide conclusions on compliance with laws and regulations. Our review disclosed no instances where KPMG did not comply, in all material respects, with generally accepted government auditing standards.

Consistent with our responsibility under the *Inspector General Act*, we are providing copies of this report to appropriate congressional committees with oversight and appropriation responsibilities over the Department. In addition, we will post a copy of the report on our public website.

We request that the Department provide us with a corrective action plan that demonstrates progress in addressing the report's recommendations.

Please call me with any questions, or your staff may contact John E. McCoy II, Acting Assistant Inspector General for Audits at (202) 254-4100 or Maureen Duddy, Deputy Assistant Inspector General for Audits, at (617) 565-8723.

Attachment

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 Financial Statements and Internal Control

We have audited the accompanying consolidated financial statements of the U.S. Department of Homeland Security (DHS or Department), which comprise the consolidated balance sheets as of September 30, 2017 and 2016, and the related consolidated statements of net cost, 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. We also have audited DHS's internal control over financial reporting as of September 30, 2017, based on criteria established in the *Standards for Internal Control in the Federal Government* issued by the Comptroller General of the United States.

Management's Responsibility for Internal Control Over Financial Reporting

Management is responsible for the preparation and fair presentation of these consolidated financial statements in accordance with U.S. generally accepted accounting principles; this includes 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 *Agency Financial Report*.

Auditors' Responsibility

Our responsibility is to express an opinion on these consolidated financial statements and an opinion on the Department's internal control over financial reporting based on our audits. We conducted our audits in accordance with auditing standards generally accepted in the United States of America, in accordance with the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States, and in accordance with Office of Management and Budget (OMB) Bulletin No. 17- 03, *Audit Requirements for Federal Financial Statements*. Those standards and OMB Bulletin No. 17- 03 require that we plan and perform the audits to obtain reasonable assurance about whether the consolidated financial statements are free from material misstatement and whether effective internal control over financial reporting was maintained in all material respects.

An audit of financial statements involves performing procedures to obtain audit evidence about the amounts and disclosures in the consolidated financial statements. The procedures selected depend on the auditors' judgment, including the assessment of the risks of material misstatement of the consolidated financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the consolidated financial statements in order to design audit procedures that are appropriate in the circumstances. An audit of financial statements also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the consolidated financial statements.

An audit of internal control over financial reporting involves performing procedures to obtain audit evidence about whether a material weakness exists. The procedures selected depend on the auditors' judgment, including the assessment of the risks that a material weakness exists. An audit of internal control over financial reporting also involves obtaining an understanding of internal control over financial reporting and testing and evaluating the design and operating effectiveness of internal control over financial reporting based on the assessed risk.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinions.

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 consolidated 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.

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 financial statements will not be prevented or detected and corrected on a timely basis. The following material weaknesses, described in Exhibit I, have been identified and included in the *Secretary's Assurance Statement*:

A. Information Technology Controls and Financial System Functionality
B. Financial Reporting

We do not express an opinion or any other form of assurance on management's evaluation and assurances made in the *Secretary's Assurance Statement*.

Opinions

In our opinion, the consolidated financial statements referred to above present fairly, in all material respects, the financial position of the U.S. Department of Homeland Security as of September 30, 2017 and 2016, 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.

Also, in our opinion, because of the effect of the material weaknesses described in Exhibit I on the achievement of the objectives of the control criteria, DHS has not maintained effective internal control over financial reporting as of September 30, 2017, 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 Exhibit I in determining the nature, timing, and extent of audit tests applied in our audit of the fiscal year 2017 consolidated financial statements, and these findings do not affect our unmodified opinion on the consolidated financial statements.

Emphasis of Matter

As discussed in Notes 1T, 15, and 25 of the consolidated financial statements, the Department had intragovernmental debt of approximately $30 billion and $23 billion used to finance the *National Flood Insurance Program* (NFIP) as of September 30, 2017 and 2016, respectively. Due to the subsidized nature of the NFIP, the Department has determined that future insurance premiums, and other anticipated sources of revenue, may not be sufficient to repay this debt. As discussed in Note 31 of the consolidated financial statements, on October 26, 2017, Congress enacted the *Additional Supplemental Appropriations for Disaster Relief Requirements Act of 2017*. This act forgives $16 billion of the Department's debt that is included in the DHS consolidated balance sheet as of September 30, 2017. Further legislation will need to be enacted to provide funding to repay or forgive the remaining debt. Our opinion is not modified with respect to this matter.

Other Matters

Agency Financial Report

We do not express an opinion or any form of assurance on management's statement referring to compliance with laws and regulations in the accompanying *Agency Financial Report*.

Internal Control Over Financial Reporting

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 following deficiencies in the U.S. Department of Homeland Security's internal control, described in Exhibit II, to be significant deficiencies:

C. Entity-Level Controls
D. Property, Plant, and Equipment
E. Custodial Activities: Entry Process and Refunds and Drawbacks
F. Grants Management

DHS's response to the findings identified in our audits is described in Appendix A. DHS's response was not subjected to the auditing procedures applied in the audit of the FY 2017 consolidated financial statements and, accordingly, we express no opinion on the response.

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 financial statements. Such information is not a required part of the basic 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.

Required Supplementary Information

U.S. generally accepted accounting principles require that the information in the Management's Discussion and Analysis, Required Supplementary Information, and Required Supplementary Stewardship Information sections be presented to supplement the basic consolidated financial statements. Such information, 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 auditing standards generally accepted in the United States of America, 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

Our audits of the consolidated financial statements were conducted for the purpose of forming an opinion on the basic consolidated financial statements as a whole. The information in the Message from the Secretary, Message from the Chief Financial Officer, and Other Information section, as listed in the Table of Contents of the *Agency Financial Report*, is presented for purposes of additional analysis and is not a required part of the basic consolidated financial statements. Such information has not been subjected to the auditing procedures applied in the audits of the basic consolidated financial statements, and accordingly, we do not express an opinion or provide any assurance on it.

Other Reporting Required by *Government Auditing Standards*

Compliance and Other Matters

As part of obtaining reasonable assurance about whether DHS's consolidated financial statements 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 determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit of the FY 2017 consolidated financial statements, and accordingly, we do not express such an opinion. The results of our tests of compliance disclosed the following instances of noncompliance or other matters that are required to be reported herein under *Government Auditing Standards* or OMB Bulletin No. 17-03, and which are described in Exhibit III:

G. *Federal Managers' Financial Integrity Act of 1982*
H. *Single Audit Act Amendments of 1996*
I. *Antideficiency Act*

We also performed tests of its 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 of the FY 2017 consolidated financial statements, and accordingly, we do not express such an opinion. The results of our tests of FFMIA disclosed instances, as described in finding J of Exhibit III, where DHS's financial management systems did not substantially comply with the (1) Federal financial management systems requirements, (2) applicable Federal accounting standards, and (3) the United States Government Standard General Ledger at the transaction level.

***Purpose of the Other Reporting Required by* Government Auditing Standards**

The purpose of the communication described in the Other Reporting Required by *Government Auditing Standards* section is solely to describe 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, 2017

The internal control weaknesses in financial reporting, and findings related to compliance with certain laws, regulations, contracts, and grant agreements, presented herein, were identified during our audits of the U.S. Department of Homeland Security's (Department or DHS) financial statements as of September 30, 2017 and internal control over financial reporting. Our findings are presented in three Exhibits:

Exhibit I Findings that individually or in aggregate are considered material weaknesses in internal control over financial reporting affecting the DHS consolidated financial statements.

Exhibit II Findings that individually or in aggregate are considered significant deficiencies in internal control over financial reporting, which are less severe than a material weakness, yet important enough to merit attention of DHS management and others in positions of DHS oversight.

Exhibit III 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. 17-03, *Audit Requirements for Federal Financial Statements*.

Criteria *Index of Financial Reporting and Internal Control Criteria*

The determination of which findings rise to the level of a material weakness or significant deficiency is based on an evaluation of how deficiencies identified in all Components, considered in aggregate, may affect the Department's internal control over financial reporting as of September 30, 2017.

We have reported the following two material weaknesses, four significant deficiencies, and four instances of noncompliance at the Department level for FY 2017:

Material Weaknesses (Exhibit I):

Comment	Financial Statement Area
A	Information Technology Controls and Financial System
B	Financial Reporting

Significant Deficiencies (Exhibit II):

Comment	Financial Statement Area
C	Entity-Level Controls
D	Property, Plant, and Equipment
E	Custodial Activities: Entry Process and Refunds and Drawbacks
F	Grants Management

Compliance and Other Matters (Exhibit III):

Comment	Compliance Area
G	*Federal Managers' Financial Integrity Act of 1982*
H	*Single Audit Act Amendments of 1996*
I	*Antideficiency Act*
J	*Federal Financial Management Improvement Act of 1996*

The criteria supporting our findings, such as references from technical accounting standards, various rules and regulations, including requirements issued by the OMB and the U.S. Department of the Treasury (Treasury), and internal Departmental and Component directives, are presented in the *Index of Financial Reporting and Internal Control Criteria* behind Exhibit III.

All Components of DHS, as defined in Note 1A – *Reporting Entity* to the financial statements, were considered in the scope of our audits of the DHS financial statements and internal control over financial reporting.

I-A Information Technology Controls and Financial System Functionality

Background: Information technology controls are a critical subset of an entity's internal control. They are typically categorized as either general IT controls (GITCs) or business process application controls (application controls). GITCs operate over all or a large portion of systems and represent the foundation of an IT control structure. They are applied at the entity-wide, system, and application level and include controls over security management, access, configuration management, segregation of duties, and contingency planning. Effective GITCs are necessary to create the foundation for the effective operation of application controls. Application controls are those controls that directly relate to specific IT applications and ensure the complete and accurate processing of data.

During our FY 2017 assessment of GITCs, we noted DHS made some progress in remediating IT findings we reported in FY 2016: however, new findings were identified in FY 2017. Additionally, management did not take appropriate corrective action to address ongoing pervasive deficiencies that we identified in multiple information systems and reported to management as a material weakness for several years. We deemed the following internal control deficiencies to, collectively, be a material weakness in internal control over financial reporting.

Conditions Related to GITCs: The control deficiencies in GITCs represent an overall elevated risk of material misstatement as the Department lacks sufficient manual controls in process areas to fully mitigate these GITC deficiencies. Deficiencies indicated in this Exhibit are a cross-section of GITC deficiencies identified. We identified the following:

Access Controls/Segregation of Duties:

DHS did not:

- adequately and consistently design and implement controls over initial authorization and periodic recertification of application, database, and operating system user, service, and generic accounts (including emergency, temporary, developer, and migrator access) and ensure adherence to the principles of least privilege and segregation of duties.
- consistently implement technical controls over logical access to key financial applications and underlying system software components in accordance with DHS requirements. Technical controls included password and inactivity requirements and account and data protection security configurations.
- fully implement or consistently perform controls over the generation, review, analysis, and protection of application, database, and operating system audit logs.
- implement controls related to review and revocation of system access to ensure consistent and timely removal of access privileges from financial systems and general support systems for transferred and/or terminated employees and contractors.

Furthermore, some DHS Components use third-party systems for processing portions of human resource related transactions. We tested complementary user entity controls that DHS is responsible for implementing, and we identified access control failures across multiple Components.

Configuration Management:

DHS did not consistently or completely:

- develop and formally document policies and procedures for the configuration management process.
- maintain a complete and accurate listing of all implemented system changes.
- maintain documentation of configuration management changes in accordance with DHS policy.

Conditions Related to Financial System Functionality: During our audit, we also evaluated and considered the impact of financial system functionality on financial reporting. In recent years, we noted that limitations in the Department's financial systems' functionality inhibit its ability to implement and maintain effective internal control, and to effectively and efficiently process and report financial data. Many key DHS financial systems were not compliant with Federal financial management system requirements as defined by FFMIA and OMB Circular No. A-123, Appendix D, *Compliance with the Federal Financial Management Improvement Act of 1996*.

GITCs and financial process areas were implemented or supported by manual processes, decentralized systems or records management processes, or utilities with limited automated capabilities at several DHS Components. These functionality limitations introduced a high risk of error and resulted in inconsistent, incomplete, or inaccurate control execution and supporting documentation.

In addition, system limitations contributed to deficiencies identified in multiple financial process areas across the Department. For example, system configurations and posting logic deficiencies limited the effectiveness of controls to accurately record certain activity at the transaction level, identify funding variances, or prevent or detect and correct excessive drawback claims. In some cases, Components implemented manual processes to compensate for these limitations; however, these manual processes were more prone to error and increased the risk that financial data and transactions were improperly recorded in the respective systems.

Cause: The control deficiencies described in this Exhibit stem from a number of systemic root causes across the Department. In many cases, inadequately designed and implemented or ineffectively operating controls were caused by the following: resource limitations; ineffective or inadequate management oversight, awareness, and training; the complex, highly interrelated yet decentralized nature of systems and system components; a lack of communication between offices in the same organization regarding GITC ownership; a lack of continual self-review and risk assessments performed over GITCs; and/or error-prone manual processes. In some cases, cost-prohibitive options for vendor support limited system development activity to "break/fix" and sustainment activities.

Root causes related to deficient entity-level controls are further discussed in Comment **II-C**, *Entity-Level Controls*.

Effect: Deficiencies related to access controls and segregation of duties increase the risk that current employees, separated employees, or contractors may obtain unauthorized or inappropriate access to financial and support systems or data. Such access could lead to unauthorized activities or inappropriate disclosures of sensitive data. Deficiencies related to 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.

The conditions supporting our findings collectively limit the Department's ability to process, store, and report financial data in a manner that ensures accuracy, confidentiality, integrity, and availability. The aggregate impact of the GITC deficiencies result in a pervasive risk within the consolidated financial statements that a material misstatement will not be prevented or detected and corrected in a timely manner as the process level application controls that are supported by the GITCs are rendered ineffective. Ineffective process level application controls, in turn, create a need for mitigating controls which were often not present or designed, implemented, and operating at a level of precision to prevent and/or detect a material misstatement. Additionally, mitigating controls often were more manual in nature, increasing the risk of human error that could materially affect the financial statements. We identified deficiencies related to design, implementation, operating effectiveness, and lack of manual mitigating controls, which contributed to the findings reported in Exhibits I, II, and III. Furthermore, due to these GITC deficiencies, we deemed certain key manual controls throughout the Department ineffective as they are dependent upon application controls to ensure the completeness and accuracy of information personnel produced from systems for use in the operation of those manual controls.

Until DHS addresses its legacy IT issues and implements updated IT solutions, it is reliant on compensating controls and other complex manual workarounds to support its IT environment and financial reporting processes.

Criteria: We do not present relevant criteria for IT controls and financial system functionality due to the sensitive nature of the Department's systems. Relevant criteria is provided in individual limited distribution (For Official Use Only) Notices of Findings and Recommendations (NFRs) to DHS and Component management.

Recommendation:

1. We recommend that the DHS Office of the Chief Financial Officer (OCFO), in coordination with the Office of the Chief Information Officer (OCIO) and Component management, make the necessary improvements to the Department's supporting IT general controls. Specific, more detailed

recommendations were provided in individual limited distribution NFRs to DHS and Component management.

I-B Financial Reporting

Background: Financial reporting relates to the preparation of financial information for inclusion in the financial statements and related disclosures and includes the activities for initiation, authorization, recording, and processing transactions in the general ledger. It includes procedures related to the selection and application of accounting policies and management's oversight of the process.

The Department continued to implement corrective action plans and made progress in certain areas, such as the United States Coast Guard (USCG or Coast Guard) improving the design of management review controls over actuarial liabilities. Coast Guard management demonstrated greater understanding of the actuarial pension and healthcare valuation processes, including assumptions and sources of data used in the valuations. However, management needs to refine these controls. Additionally, deficiencies we identified in FY 2016 persisted, and we identified new deficiencies at United States Secret Service (USSS). We deemed the following internal control deficiencies to, collectively, be a material weakness in internal control over financial reporting:

Conditions pervasive across the Department:

- The Department lacked sufficient manual controls in process areas to fully mitigate the risks caused by GITC deficiencies.
- The Department did not maintain effective internal control related to service organizations, including evaluating and documenting the roles of service and sub-service organizations; performing effective reviews of service organization control (SOC) reports; considering and/or implementing complementary user entity controls identified in SOC reports; and assessing and addressing service provider risk in the absence of SOC reports.

Cause: The Department lacks robust continuous monitoring and testing of IT general controls necessary to identify weaknesses, assess the resulting risks created by IT deficiencies, and respond to those risks through compensating controls. The lack of compensating controls results in the Department's noncompliance with the requirements of FFMIA and OMB Circular No. A-123, Appendix D, *Compliance with the Federal Financial Management Improvement Act of 1996* as reported in Comment **III-J**, *Federal Financial Management Improvement Act of 1996* (FFMIA). Personnel tasked with evaluating the roles of service organizations and the controls at service organizations as well as complementary user entity controls within the Components relying on those service organizations often do not possess the required understanding of internal control or the related business process to perform an effective assessment.

Conditions related to the review and approval of journal entries:

- Coast Guard lacked effective controls:
  - over the review of manual adjusting journal entries to prevent and/or detect and correct financial reporting errors and to ensure activity aligned with actual current year business events.
  - to ensure accuracy of certain beginning balance and year-end close-out activities, at the transaction level, in its three general ledgers due to on-top adjustments for all activity only being recorded to one general ledger.
- CBP did not have effective controls related to the preparation and review of manual entries, including underlying information. Specifically:
  - Management lacked effective controls over manual journal entries related to the reporting of cash collections on the statement of custodial activity.
  - Management recorded manual budget entries in the general ledger without appropriate supporting documentation.

- USSS did not design and implement effective controls over the review and approval and related segregation of duties of manual journal entries. Specifically:
  - Management recorded several journal entries directly to DHS Treasury Information Executive Repository (the central repository for key financial management information for DHS Components), for which support did not exist and approval was not evidenced.
  - Management did not record entries related to the pension liability and expense for the proper amounts or to the proper standard general ledger accounts.

Cause: The Coast Guard's three legacy general ledger systems, developed over a decade ago, have severe functional limitations and necessitate large manual adjusting entries to compensate for the ability to record transactions correctly upon initiation. The magnitude of these entries inhibit management from performing adequate reviews of activity for reasonableness and alignment with current year business events. These system functionality limitations also hinder Coast Guard's ability to ensure accuracy of certain beginning balance and year-end close-out activities. Also refer to IT financial system functionality issues described at Comment **I-A**, *Information Technology Controls and Financial System Functionality.* Due to high turnover of key financial management personnel and the lack of well-defined policies and procedures, USSS personnel lacked sufficient knowledge to properly perform the review and approval of manual journal entries. CBP personnel also lacked sufficient knowledge to properly perform the review and approval of manual entries, primarily due to a lack of adequate training and coordination with financial reporting personnel.

Conditions related to actuarially derived estimates:

- Coast Guard did not sufficiently design, implement, or adequately document:
  - management's review of relevant assumptions, specifically related to newly developed internal experience studies, used in the valuation of the actuarial pension and healthcare liabilities.
  - management's review of the actuary-prepared valuation reports for the pension and healthcare liabilities to include sufficiently precise review thresholds in which to evaluate the impact of changes in assumptions on the valuation results and reconciling underlying report data.
  - controls to reconcile medical claims data to ensure completeness and accuracy of the underlying data prior to submission of the data to the external actuary for use in the valuation of the actuarial healthcare liability.
- USSS did not fully assess risk, design and implement sufficient controls, and document processes over its actuarial pension liability. Specifically, management did not:
  - implement sufficient controls for management review of assumptions used in the valuation of the liability.
  - implement policies and procedures to document their consideration and assessment of estimation uncertainty; contradictory evidence; continued appropriateness of assumptions and estimation methodology; and retrospective review of assumptions and normal cost associated with the plan.
  - implement controls to validate the completeness and accuracy of underlying data used in the valuation of the liability.

Cause: Coast Guard made improvements in internal control related to actuarial liabilities, yet management did not fully understand the extent of their internal control responsibilities. Management did not appropriately document and perform to a sufficient level of precision its review controls related to the estimates. USSS management did not possess a sufficient understanding of the USSS actuarial pension valuation process to fully assess the appropriateness of the assumptions due to over reliance on an external actuary. In addition, existing policies and procedures were not sufficiently specific to enable new employees to review census data changes or complete the annual review checklist.

Other financial reporting related conditions:

- Coast Guard lacked controls to reconcile intra-governmental activities and balances and ensure that transactions were recorded to the correct trading partner at the time the business event occurred.

- USSS did not establish an accrual methodology to properly recognize and record expenses and accounts payable within the period the goods or services were delivered or received.
- USSS lacked properly designed and implemented controls over the preparation and review of periodic financial information at an appropriate level of precision in various processes, including payroll and budgetary obligations and transactions (see also **Comment II-D**, *Property, Plant, and Equipment*).

Cause: Financial system functionality issues also hindered Coast Guard's ability to ensure that transactions were recorded to the correct trading partner at the time of the business event, which, in turn, impacted their ability to reconcile intra-governmental activities and comply with relevant Federal financial system requirements and guidelines as noted in Comment **III-J**, *Federal Financial Management Improvement Act of 1996* (FFMIA). Also refer to IT financial system functionality issues described at Comment **I-A**, *Information Technology Controls and Financial System Functionality.* Due to high turnover of key financial management personnel and the lack of well-defined policies and procedures, USSS personnel lacked sufficient knowledge and an effective communication structure to carry out critical financial reporting functions.

Root causes related to deficient entity-level controls are further discussed in Comment **II-C**, *Entity-Level Controls*.

Effect: The aggregate impact of the financial reporting deficiencies result in a pervasive risk across the consolidated financial statements that a material misstatement will not be prevented or detected and corrected in a timely manner.

Criteria: Presented in *Index of Financial Reporting and Internal Control Criteria,* after Exhibit III.

Recommendations: We recommend that:

DHS:

2. develop continuous monitoring and testing of IT general controls to identify weaknesses, assess the resulting risks created by any identified IT deficiencies, and respond to those risks through implementing compensating controls.
3. align knowledgeable resources to 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.

Coast Guard:

4. improve and reinforce existing policies, procedures, and related internal controls to ensure that:
    a. management adequately researches, supports, and reviews all journal entries and adjusting entries prior to recording in the general ledger.
    b. management records approved on top adjustment entries in the correct underlying general ledger systems in order to generate accurate beginning balances.
    c. personnel record transactions to the accurate trading partner upon initiation; reconcile all intra-governmental balances with trading partners; and resolve differences in a timely manner.
    d. management enhances documentation of their actuarial liability estimate reviews and refines their review of the actuarial liabilities report, underlying data, and assumptions to include precise reconciliations and thresholds.

USSS:

5. establish new, or improve existing, policies, procedures, and related internal controls over the valuation of its pension liability to ensure:
    a. personnel adequately understand the pension estimate.
    b. management maintains oversight of assumptions used in significant estimates and routinely evaluates continued appropriateness of those assumptions.

   c. management completes the annual pension checklist.
   d. management reviews the underlying census data at least annually.

6. develop and implement policies and procedures over the review of manual journal entries.
7. develop and implement policies and procedures for an accrual methodology.
8. design and implement controls over the preparation and review of periodic financial information.

CBP:

9. provide additional training to individuals who prepare and review manual entries that emphasizes the impact of entries on the reporting of financial information.

II-C Entity-Level Controls

Background: Entity-level controls are controls that have an overarching or pervasive effect on an entity. They include the entity's culture, values, and ethics, as well as the attitudes, awareness, and actions of management and those charged with governance concerning the entity's internal control. Entity-level controls reside in all five components of internal control – control environment, risk assessment, control activities, monitoring, and information and communications – as defined by the *Standards for Internal Control in the Federal Government* issued by the Comptroller General of the United States. These controls must be effectively designed, implemented, and operating together in an integrated manner to create and sustain an organizational structure that is conducive to reliable financial reporting.

The conditions below should be read in conjunction with Comment **I-A**, *Information Technology Controls and Financial System Functionality*; Comment **I-B**, *Financial Reporting*; Comment **II-D**, *Property, Plant, and Equipment*; Comment **II-E**, *Custodial Activities: Entry Process and Refunds and Drawbacks*; and Comment **II-F**, *Grants Management*.

Conditions, Cause/Effect, and Recommendations: During our audit we identified certain control deficiencies for which underlying causes were similar and pervasive throughout the Department. The resulting recommendations, which we provided to correct the deficiencies, are based on improvements needed in management's control environment, risk assessment process, communication practices throughout the Department, and its monitoring activities. Without improvements in these areas, management will be unable to overcome long-standing internal control weaknesses. Accordingly, we deemed the entity-level control deficiencies described below to, collectively, merit the attention of those charged with governance.

Control Environment: The Department has established an organizational structure and assigned responsibilities in a manner to allow Components to operate efficiently and effectively to achieve their objectives. As such, internal control responsibilities are assigned to Components that are responsible for establishing an internal control system at the Component level. Individual Components have differing levels of control environment effectiveness. Additional Department-level leadership is required to address the following areas of the control environment at certain components:

10. filling needs for technical and resource personnel support to remediate severe control deficiencies or prevent deterioration of the internal control system.
11. assessing training needs for personnel and aligning skills with roles and responsibilities; and ensuring individuals in key roles with internal control responsibilities possess the appropriate competencies to perform their duties and are held accountable for their internal control responsibilities.
12. ensuring significant accounting policies and standard operating procedures are formally documented, complete, updated, and revised timely.
13. defining roles and responsibilities of program and field personnel that provide key financial information, and ensuring those personnel understand and comply with policies.
14. establishing a structure with central ownership and oversight for internal controls where responsibilities have been delegated to discrete units.
15. defining succession and contingency plans for key roles involved in internal control over financial reporting to mitigate risks due to employee turnover.

Risk Assessments: The Department has not fully matured its risk assessment processes. As a result, events and transactions that have a greater likelihood of error do not always receive an appropriate level of attention. Risk assessments should be enhanced at both the headquarters level by Departmental management, and individual Components annually, and updated during the year as needed. Examples of areas that should be analyzed and responded to accordingly to enhance the risk assessments include:

16. planned changes that could impact the internal control system, such as financial system transitions and implementation of new tools.
17. processes reliant on information from service organizations, and effectiveness of controls operating at those service organizations.

18. processes and controls in which management relies on system generated or manually prepared reports to respond to risk of incomplete or inaccurate information within those reports.
19. financial accounts and transactions that are susceptible to error due to IT systems functionality issues and inability to rely on application controls supported by IT general controls that are deficient. Refer to Comment **I-A**, *Information Technology Controls and Financial System Functionality*.

Information and Communications: Communications within Components, between headquarters and Components, and between financial and IT management, should be improved to ensure:

20. coordination between headquarters and Components with resource constraints to respond to financial accounting and reporting risks and control deficiencies.
21. the structure, process, and communication between key stakeholders is sufficient to ensure there is a complete understanding of the end-to-end flow of transactions for key business processes that impact financial reporting.
22. individuals within the financial reporting, accounting and budget departments identify and use quality information for financial reporting.
23. roles and responsibilities of program and field personnel that provide key financial information are communicated, and that those personnel understand and comply with policies.
24. individuals with key internal control responsibilities have a sufficient understanding of the implication of IT vulnerabilities and limitations, and manual compensating internal controls are designed and implemented to mitigate risk.
25. monitoring across larger Components with decentralized operations to ensure responsibilities have been properly assigned and clearly communicated, and that internal control over financial reporting and compliance with direct and material laws and regulations have been properly designed and implemented and are operating effectively across the organization.

Monitoring Controls: As a result of its monitoring activities, which included executive level support, the Department continued to make progress in identifying and remediating control deficiencies in certain areas. However, the Department did not effectively monitor the implementation of corrective actions for all reportable deficiencies identified in the prior year. Additionally, Component management did not always design detective controls (e.g., management review controls of the financial statements) to a proper level of precision to compensate or mitigate weak preventative or process level controls. Consequently, errors, or a combination of errors, in the financial statements could go undetected. These conditions also impact compliance with the *Federal Managers' Financial Integrity Act of 1982*, as cited in Comment **III-G**.

We recommend that DHS:

26. design continuous monitoring controls to ensure personnel with internal control oversight responsibilities adequately examine transactions with a higher risk of error.
27. seek opportunities to implement more reliable controls earlier in the process to prevent errors at the transaction source.
28. enhance internal testing of both financial and IT controls to identify and remediate deficiencies as they may arise in order to sustain auditable financial statements in the future.

II-D Property, Plant, and Equipment

Background: In FY 2017, the Coast Guard and the National Protection and Programs Directorate (NPPD) made significant improvements in demonstrating the design and operating effectiveness of internal controls over PP&E. Specifically related to USCG, which comprises over half of the DHS consolidated PP&E balance, we noted improvement in management's establishment of internal controls related to PP&E and alignment of these responsibilities to personnel in key roles with the appropriate expertise for performing the related control activities. NPPD implemented controls to ensure proper classification of expenditures as capital or expense and to track asset activity at a transaction level to ensure proper recording of asset activity. Though some control deficiencies identified in FY 2016 at NPPD related to PP&E persisted, we did not deem the deficiencies warranted the attention of those charged with governance.

USSS, however, continued to experience significant issues in their design and implementation of PP&E controls. USSS property primarily consists of equipment used to protect national leaders, visiting heads of state and governments, designated sites, and national special security events. USSS property also consists of buildings and leasehold improvements related to field offices and its headquarters.

Conditions: We determined the following remaining deficiencies at USCG, considered in aggregate with the following deficiencies at USSS, to merit the attention of those charged with governance:

Coast Guard did not:

- incorporate precise thresholds in their design and implementation of controls over the management review of the construction-in-progress (CIP) rollforward schedule of activity in order to appropriately evaluate the validity of activity and ensure alignment with business events.
- effectively design and implement control procedures over management's review of the classification of CIP costs to ensure a sufficient number of cost decisions are reviewed to identify and evaluate any pervasive inaccuracies in the underlying allocation.
- effectively design and implement controls over the physical count of real property assets to ensure assets are sufficiently inventoried such that assets which are no longer functional are timely identified and impaired.
- have controls that were operating effectively over the timely recording of fixed asset addition and retirement activity in the general ledger.

USSS did not:

- design and implement controls and processes to reconcile its PP&E detailed sub-ledger to the general ledger.
- implement established inventory policies and control procedures to ensure the completeness, existence, and accuracy of real and personal property assets.
- design and implement sufficient controls to appropriately track asset activity at a transaction level, and ensure the timely recording of asset additions, deletions, or other adjustments to PP&E.
- design and implement controls and processes to identify instances of and criteria for asset impairment.

Cause: During FY 2017, Coast Guard utilized a risk based approach to remediation of control deficiencies that prioritized the refinement of the design, development, and implementation of control processes related to monitoring of PP&E. However, management lacked an appropriate level of precision to sufficiently evaluate all CIP activity and did not focus efforts on remediation of deficiencies related to real property inventories and the timely recording of asset activity.

USSS did not properly assess the risks and implement controls related to the capital property processes, including proper integration between the sub-ledger and general ledger. USSS did not have the appropriate resources to monitor and oversee the reporting and recording of capital property. Additionally, the Administrative Operations Division and the Financial Management Division did not communicate sufficiently to ensure proper accountability. As a result, USSS experienced significant difficulties in providing complete and accurate data to support operating controls and year-end PP&E balances.

Root causes related to deficient entity-level controls are further discussed in Comment **II-D**, *Entity-Level Controls*.

Effect: The aggregate impact of the PP&E deficiencies result in a risk that misstatements related to the completeness, existence, and valuation of PP&E are not prevented and/or detected and corrected in a timely manner.

Criteria: Presented in *Index of Financial Reporting and Internal Control Criteria,* after Exhibit III.

Recommendations: We recommend that:

Coast Guard:

29. enhance controls over the management review of the CIP rollforward to ensure validity of activity within defined thresholds and accurate recording in the general ledger.
30. further develop the design of controls over the review of CIP activity cost decisions to ensure a sufficient number of review is completed.
31. refine the design of controls over the physical count of real property assets to ensure the completeness and existence of all real property assets.
32. reinforce controls over the timely recording of asset addition and retirement activity.

USSS:

33. design and implement controls and procedures to perform reconciliations between the PP&E sub-ledger to the general ledger and reconcile all significant differences.
34. adhere to established inventory policies and procedures, and design and implement controls to appropriately track asset activity at the transaction level and ensure the timely recording of asset additions, deletions, or other adjustments.
35. establish new, or improve current, communication channels and standard operating procedures within the Administrative Operations Division and Financial Management Division to ensure sufficient review of personal and real property activity and balances, including equipment, internal-use software, land, buildings and other structures, and to verify costs are appropriate and reflect USSS's business operations during the fiscal year.
36. design and implement controls and processes to identify instances and criteria for asset impairment.
37. attract and deploy additional skilled resources within the Administrative Operations Division and Financial Management Division to support the control environment and provide the necessary financial reporting oversight.

II-E Custodial Activities: Entry Process and Refunds and Drawbacks

Background: CBP comprises approximately 99% of the Department's custodial activities. The majority of CBP's custodial collections are from merchandise entering the United States from foreign ports of origin, against which CBP assesses import duties, taxes, and fees. Receipts of import duties and disbursement of refunds are presented on the statement of custodial activity. Any taxes, duties and trade receivables (TDTR) related to merchandise that has entered commerce but has not been collected is recorded on the DHS balance sheet as TDTR. TDTR also includes any fines and penalties and supplemental duty bills, including anti-dumping and countervailing duties that CBP has assessed against the trade due to non-compliance with trade laws. To ensure the subsequent collection of these unpaid duties, taxes and fees, CBP requires bonds from parties that import merchandise into the United States. The assessment of liquidated damages against a bond serves to promote compliance with laws and regulations (identified as the entry process).

Drawback claims are a remittance, in whole or in part, of duties, taxes, or fees previously paid by an importer. Drawback claims typically occur when imported goods on which duties, taxes, or fees have been previously paid are subsequently exported from the United States or destroyed prior to entering the commerce of the United States. The *Trade Facilitation and Trade Enforcement Act of 2015* (TFTEA) contained provisions for drawback modernization that simplify the rules for determining if exports are eligible for drawback refunds, expand the timeframe for drawback claims, and eliminates some of the documentation requirements.

Many of the conditions cited below have existed for several years. Management has stated that the timeframe for remediation of these conditions is dependent on successful implementation of IT system upgrades and the TFTEA legislation changes.

Conditions: We identified the following internal control deficiencies related to custodial activities at CBP that we deemed to, collectively, merit the attention of those charged with governance:

Related to the Entry Process:

- CBP did not clearly establish consistent procedures for completing and documenting the review of the entry edit and exception reports. Port personnel performed and documented their reviews inconsistently from port to port and did not consider the completeness and accuracy of the data used in the performance of the controls. Additionally, port personnel did not subject items that have been reviewed or prepared by a Center of Excellence and Expertise to the same level of review as those items that were prepared by the port.
- Port personnel did not effectively review the sufficiency of bonds used for entry by importers and brokers. Specifically, management was unable to demonstrate that port personnel reviewed Single Transaction Bonds (STBs) for sufficiency.
- The automated control designed to monitor the sufficiency of continuous bonds did not accurately capture necessary financial data to ensure the sufficiency of those bonds.
- CBP did not properly design controls to ensure the proper recording of fines, penalties and forfeitures (FP&F) related to TDTR and the associated allowance balance. Specifically, CBP did not have a consistently executed process to update receivable amounts for offers in compromise or mitigated receivables.
- CBP did not properly design controls to ensure the timely resolution of liabilities for deposit accounts, which are reported as part of other non-governmental liabilities on the balance sheet. Specifically, CBP did not have a consistently executed process to recognize prior disclosures and other deposits as custodial revenue once a specifically identifiable, legally enforceable claim to the deposit arises.

Related to Refunds and Drawbacks:

- The current refunds and drawbacks IT system lacked effective automated controls to prevent, or detect and correct, excessive drawback claims. The programming logic did not link drawback claims to imports at a sufficiently detailed level. In addition, the system did not have the capability to compare, verify, and track essential information on drawback claims to the related underlying consumption entries and export documentation upon which the drawback claim was based. Further, the system had not been configured to restrict drawback claims to 99 percent of each entry summary, in accordance with regulations for applicable drawback claims.
- Manual drawback review policies did not require drawback specialists to review prior drawback claims at a sufficient level of detail against a selected import entry to determine whether, in the aggregate, an excessive amount was claimed against import entries.
- Documentation retention periods were not appropriate to ensure that importers maintained support for drawback transactions for the full claim time-period and CBP maintained support for importers qualifying for accelerated filer status.
- Automated controls did not operate effectively to prevent a claimant from exceeding the continuous bond amount on file.

Cause/Effect: Policies and procedures over the review of entry edit, and exception reports were not sufficiently to ensure personnel performed the controls consistently at all ports and Centers of Excellence and Expertise during FY 2017. In addition, existing policies and procedures do not require timely coordination with all applicable parties. Failure to consistently adhere to existing policies and procedures for review and verification of reports may result in a potential misstatement to the balance of net TDTR and total cash collections on the statement of custodial activities. Inadequate controls could result in CBP's failure to identify amounts that are due to the Treasury general fund.

CBP did not consistently adhere to policies and procedures for the review of STBs; and CBP management did not develop and communicate policies and procedures to uniformly perform and document the manual review of STBs for sufficiency. The mandated timeframe for the transition from CBP's legacy to new entry system and resource constraints prevented CBP from fully developing policies and procedures before implementing operational changes. Additionally, resource constraints inhibited management's ability to timely remediate the monitoring of continuous entry bonds.

Failure to fully establish and define control environments related to the entry process, including FP&F and liability for deposit accounts, could lead to potential misstatements of net TDTR and other non-governmental liabilities on the DHS balance sheet and total cash collections on the statement of custodial activities.

IT system functionality and outdated IT systems contribute to the weaknesses identified above. Refer to Comment **I-A**, *Information Technology Controls and Financial System Functionality*. The Automated Commercial System (ACS) does not provide the necessary functionality to prevent the overpayment of drawback claims. CBP plans to replace its drawback system in the future. However, until such implementation occurs, CBP does not currently have sufficient resources to effectively perform compensating manual controls over drawback claims. TFTEA changes the statutes that govern the drawback process and further reduces the need for manual controls. However, it does not take effect until February 2018. The length of the drawback claim lifecycle often extends beyond the documentation retention period, which is set by statute. Until effective automated and manual controls are implemented over the drawback process, CBP may be subject to financial loss due to excessive drawback claims. In addition, drawback claims are governed by the laws and regulations in effect at the time of filing. As the length of the drawback lifecycle can last several years, it will take several years for claims existing prior to the implementation of TFTEA to be completed.

Criteria: Presented in *Index of Financial Reporting and Internal Control Criteria,* after Exhibit III.

Recommendations: We recommend that CBP:

Related to the Entry Process:

38. update and redistribute guidance to appropriate personnel regarding the relevant CBP directives to ensure consistent performance of controls across all locations and provide training to all personnel on new policies to ensure consistent implementation at decentralized locations.
39. develop policies and procedures to ensure that each STB is reviewed for sufficiency until automation occurs.
40. fully implement the automated controls over continuous transaction bond processing.
41. enhance policies and procedures over the review of FP&F and liability for deposit account balances to ensure balances are properly stated at year-end.

Related to Refunds and Drawbacks:

42. continue with the scheduled implementation of the new drawback system.
43. implement requirements of TFTEA, which will take effect beginning in February 2018.
44. continue to enhance the manual controls to prevent, or detect and correct excessive drawback claims after the implementation of TFTEA, as current claims will take several years to be processed through the drawback lifecycle.
45. implement policies and procedures to ensure supporting documentation for accelerated filer status is maintained.

II-F Grants Management

Background: The Federal Emergency Management Agency (FEMA) is the primary grantor within DHS, managing multiple Federal disaster and non-disaster grant programs.

Conditions: The majority of the following internal control deficiencies related to grants management were reported in the prior year and persisted in FY 2017. We deemed these deficiencies to, collectively, merit the attention of those charged with governance.

FEMA did not:

- effectively communicate policies and procedures to the regional offices, where the majority of day-to-day management of its grantees occurs, to ensure that internal controls over the monitoring of grantees' compliance with laws and regulations had been properly designed and implemented, and were operating effectively.
- issue Management Decision Letters timely for single audit reports available in the Federal Audit Clearinghouse.
- reconcile grantee quarterly financial reports to FEMA's systems consistently and effectively.
- consistently implement effective controls to ensure timely closeout of FEMA's grants.

Cause/Effect: FEMA did not fully implement policies and procedures over its grant program in order to ensure compliance with the *Single Audit Act*, as implemented by the Super Circular. In addition, FEMA did not have a grants IT system in place to efficiently and comprehensively track grants to help ensure that all programmatic events were accurately and timely completed and properly recorded to the general ledger. Manual processes, which were not always effective, were used to reconcile open grants within grants systems to FEMA's general ledger system, and to track grants eligible for close-out. Refer to Comment **I-A**, *Information Technology Controls and Financial System Functionality*. Although responsibilities surrounding grants management have been assigned to discrete units within the organization, there is no overall central oversight to ensure the delegated responsibilities are being effectively carried out for all grants. Thus, FEMA cannot ensure there is effective management and administration of the grants process, as well as compliance with provisions of the *Single Audit Act*. Specifically, the lack of standardized internal controls within FEMA caused difficulty in assembling a comprehensive status of the cash on hand at grantees and the status of grants eligible for close-out, which creates risk of excessive cash on hand at grantees and untimely closure of grants.

Criteria: Presented in *Index of Financial Reporting and Internal Control Criteria,* after Exhibit III.

Recommendations: We recommend that FEMA:

46. assign the responsibility for central oversight of grants management to one program office within FEMA.
47. complete the implementation of policies and procedures to ensure full compliance with the *Single Audit Act* related to receipt and review of grantees' single audit reports.
48. implement monitoring procedures over obtaining, reviewing timely, and reconciling required quarterly grantee reports.
49. develop and implement procedures to reconcile grant award information maintained in grant IT systems to the general ledger.
50. develop and implement procedures to create and track comprehensive lists of FEMA grants that are eligible for close-out.
51. implement a continuous quality assurance and grants monitoring process to include review of corrective actions resulting from implementation of the above recommendations.

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

FMFIA requires agencies to establish effective internal control and financial systems and to continuously evaluate and assess the effectiveness of their internal control. DHS's implementation of OMB Circular No. A-123 facilitates compliance with the FMFIA. DHS has implemented a multi-year plan to achieve full assurance on internal control. However, the DHS *Secretary's Assurance Statement* dated November 14, 2017, as presented in *Management's Discussion and Analysis* of the Department's FY 2017 *Agency Financial Report* (AFR), acknowledged the existence of material weaknesses, and therefore provided qualified assurance that internal control over financial reporting was operating effectively as of September 30, 2017. Management's findings were similar to the control deficiencies we have described in Exhibits I and II. However, continuous monitoring and testing of both financial and IT controls was not performed over all significant areas.

While we noted the Department progressed toward full compliance with FMFIA and OMB Circular No. A-123, the Department did not fully established effective systems, processes, policies, and testing procedures to ensure that internal controls are operating effectively throughout the Department. We also noted deficiencies related to monitoring of the internal control system as discussed in Comment **II-D**, *Entity-Level Controls*.

Recommendation: We recommend that the Department:

52. continue its corrective actions to address internal control deficiencies in order to ensure full compliance with FMFIA and its OMB Circular No. A-123 approved plan in FY 2018.
53. conduct complete risk assessments to identify significant risk areas and continuously monitor and test the financial and IT controls within those areas.

III-H *Single Audit Act Amendments of 1996* (Single Audit)

FEMA is the primary grantor in DHS, managing multiple Federal disaster and non-disaster grant programs. The *Single Audit Act Amendments of 1996*, as implemented by Title 2 of the Code of Federal Regulations (CFR), Part 200 - *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards* (Super Circular), requires agencies awarding grants to monitor their grantees; ensure they receive grantee reports timely; and follow-up on single audit findings to ensure that grantees take appropriate and timely action. Although FEMA monitors grantees and their single audit findings, FEMA did not fully comply with provisions in the Super Circular in FY 2017. We noted that FEMA did not review all grantee single audit reports in a timely manner. Further, the decentralization of grants management prevents FEMA from being effectively able to monitor its grantees' compliance with applicable laws and regulations.

Recommendation: We recommend that FEMA:

54. implement the recommendations in Comment **II-F**, *Grants Management*.

III-I *Antideficiency Act* (ADA)

Various management reviews and DHS Office of Inspector General (OIG) investigations are ongoing within the Department, which have or may identify ADA violations, as follows:

- The independent investigation, at the Office of Intelligence and Analysis, related to the obligation of funds in excess of its continuing resolution apportionment in FY 2012 has been completed. The package to notify the President, Congress, and the U.S. Government Accountability Office (GAO) of the violation is pending OMB clearance.
- In FY 2016, Immigration and Customs Enforcement (ICE) finalized its investigation of payments made from FY 2003 to FY 2013 exceeding statutory authority for continuing to provide medical care for detainees released from custody. The package to notify the President, Congress, and GAO of the violation is pending OMB clearance.
- In FY 2015, the Management Directorate completed the investigation of an over-obligation of funds that occurred in FY 2013. In FY 2017, DHS formally notified the President, Congress, and GAO of the violation.

- CBP is investigating a potential ADA violation related to overtime in excess of the annual cap established in the FY 2014 and FY 2015 appropriations acts. CBP is still working on corrective actions to finalize the report.
- DHS is investigating potential ADA violations related to 150 contracts and Other Transaction Agreements awarded from FY 2010 to FY 2016 (five with USCG, one with ICE, one with CBP, 36 with the Management Directorate, and 107 with the Transportation Security Administration) without the appropriate Congressional notification for awards greater than $1 million.
- USSS is investigating a potential incident related to accepting voluntary services in violation of the ADA in FY 2014.
- ICE completed its investigation of a potential ADA violation related to FY 2016 expenditures made for improvements to the ICE Director's office in excess of $5,000 without proper Congressional notification. The package to notify the President, Congress, and GAO of the violation is being prepared for routing to OMB for clearance.

Recommendation: We recommend that DHS:

55. complete the internal reviews currently planned or being performed, and properly report the results in accordance with the ADA, where necessary.

III-J *Federal Financial Management Improvement Act of 1996* (FFMIA)

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 United States Government Standard General Ledger (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.

Multiple Components did not fully comply with at least one of the requirements of FFMIA based on criteria set forth in OMB Circular No. A-123, Appendix D, C*ompliance with the Federal Financial Management Improvement Act of 1996*. The reasons for noncompliance are reported in Exhibits I and II. The DHS Secretary stated in the *Secretary's Assurance Statement,* dated November 14, 2017, that the Department's financial management systems do not substantially conform to government-wide requirements mandated by FFMIA. The Department's remedial actions and related timeframes are also presented in the FY 2017 AFR.

An element within FFMIA, Federal system requirements, is ensuring security over financial management information. This element is addressed further in the *Federal Information Security Modernization Act of 2014* (FISMA). FISMA requires the head of each agency to be responsible for: (1) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of (i) information collected or maintained and (ii) information systems used or operated; (2) complying with the requirements of the Act and related policies, procedures, standards, and guidelines, including (i) information security standards under the United States Code, Title 40, Section 11331, and (ii) information security standards and guidelines for national security systems; and (3) ensuring that information security management processes are integrated with agency strategic and operational planning processes.

We also noted weaknesses in financial systems security, reported by us in Comment **I-A**, *Information Technology Controls and Financial System Functionality*, which impact the Department's ability to fully comply with FISMA.

Recommendation: We recommend that DHS:

56. improve its financial management systems to ensure compliance with FFMIA, and implement the recommendations provided in Exhibits I and II.

Criteria	Reference
I-A Information Technology Controls and Financial System Functionality	
CBP *2013 Drawback Handbook*, Issued (HB 3700-01B)	Section 5.2
CBP Directive 5610-004B, *Resolving Certain ACS Exception and Error Reports*	Section 5.4, 5.6, & 5.11
CBP Directive No. 5610-004B, *Budget Clearing Account (BCA) and Suspense Item Report* (ACSR-CL-800) Attachment	Part 8
Code of Federal Regulations, Title 19	§113.13, §113.65, §191.51, & §191.92
Federal Financial Management Improvement Act of 1996	Section 803
Federal Managers' Financial Integrity Act of 1982	Section 2
GAO *Financial Management FFMIA Implementation Critical for Federal Accountability (GAO-02-29)*	Page 1, Paragraph 2
GAO *Standards for Internal Control in the Federal Government* (GAO-14-704G)	Overview Section 1 & 2 Principle 10, 11, 12, & 16
OMB Circular No. A-136, *Financial Reporting Requirements*, Revised	Section V
OMB Memorandum M-13-23, *Appendix D to Circular No. A-123, Compliances with the Federal Financial Management Improvement Act of 1996*	Section 7
Treasury Financial Manual Bulletin No. 2017-07, *USSGL Supplement Part I: FY2017 Reporting*	Section IV
Treasury Financial Manual Chapter 4700, *Agency Reporting Requirements for the Financial Report of the United States Government*	Section1 & 2
US Code Title 31, Chapter 15	§1501
I-B Financial Reporting	
Code of Federal Regulations, Title 5	§1315
Component Requirements Guide for Financial Reporting in FY 2017, Version 1.0	Sections 7 – 9
Federal Financial Management Improvement Act of 1996	Section 803
GAO Federal Information System Controls Audit Manual (GAO-09-232G)	Section 2 & 4

Index of Financial Reporting and Internal Control Criteria

(Listed by Exhibit, Alphabetically)

Criteria	Reference
GAO *Financial Management FFMIA Implementation Critical for Federal Accountability (GAO-02-29)*	Page 1, Paragraph 2
GAO *Standards for Internal Control in the Federal Government* (GAO-14-704G)	Overview Section 1, 2, & 4 Principles 2 - 4, 7, 9 - 14, 16, & 17
NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*	Chapter 2
OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget*	Section 120, Appendix F
OMB Circular No. A-136, *Financial Reporting Requirements*, Revised	Section V
OMB Memorandum M-13-23, *Appendix D to Circular No. A-123, Compliances with the Federal Financial Management Improvement Act of 1996*	Section 7
OMB Memorandum M-16-17, *OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control*	Section III
OMB, 2 CFR Chapter I, and Chapter II, Parts 200, 215, 220, 225, and 230, *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards*	§ 200.513
Statement of Federal Financial Accounting Standards 5: *Accounting for Liabilities of the Federal Government*	Summary, Paragraphs 22 & 67
Statement of Federal Financial Accounting Standards 7: *Accounting for Revenue and Other Financial Sources and Concepts for Reconciling Budgetary and Financial Accounting*	Paragraph 79
Statement of Federal Financial Accounting Standards 33: *Pensions, Other Retirement Benefits, and Other Postemployment Benefits: Reporting the Gains and Losses from Changes in Assumptions and Selecting Discount Rates and Valuation Dates*	Summary, Paragraph 33
Treasury Financial Manual Bulletin No. 2017-07, *USSGL Supplement Part I: FY2017 Reporting*	Section III & IV
Treasury Financial Manual Chapter 4700, *Agency Reporting Requirements for the Financial Report of the United States Government*	Section 1 & 2

Criteria	Reference
US Code Title 31, Chapter 15	§1501, §1554
II-C Entity-Level Controls	
Component Requirements Guide for Financial Reporting in FY 2017, Version 1.0	Section 3 & 8
DHS Management Directive System, MD 1030, *Corrective Action Plans*	Section VI
Federal Financial Management Improvement Act of 1996	Section 803
GAO *Standards for Internal Control in the Federal Government* (GAO-14-704G)	Section 1, 2, & 4 Principle 2 - 5, 7, 9-10, 12 - 14, 16, & 17
NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*	Chapter 2
OMB Circular No. A-50, *Audit Follow Up*	Section 1 & 5
OMB Memorandum M-16-17, *OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control*	Section III
Statement of Federal Financial Accounting Standards 5: *Accounting for Liabilities of the Federal Government*	Summary, Paragraph 67
Statement of Federal Financial Accounting Standards 33: *Pensions, Other Retirement Benefits, and Other Postemployment Benefits: Reporting the Gains and Losses from Changes in Assumptions and Selecting Discount Rates and Valuation Dates*	Summary, Paragraph 33
II-D Property, Plant, and Equipment	
Federal Financial Management Improvement Act of 1996	Section 803
GAO *Standards for Internal Control in the Federal Government* (GAO-14-704G)	Section 1 Principle 3, 5, 10, 12, 13, & 16
OMB Circular No. A-136, *Financial Reporting Requirements*, Revised	Section II
Statement of Federal Financial Accounting Standards 6: *Accounting for Property, Plant, and Equipment*	Paragraph 39
USCG, Audit Remediation Division (CG-845), *Interim Standard Operating Procedure, CG-845 Construction-in-Progress Monthly Periodic Review Process*	Section 5

Criteria	Reference
USCG, *Financial Resource Management Manual - Procedures*, COMDTINST M7100.4	Section 7 & 10
II-E Custodial Activities: Entry Process and Refunds and Drawbacks	
CBP *2013 Drawback Handbook*, Issued (HB 3700-01B)	Section 5
CBP Directive 5610-004B, *Resolving Certain ACS Exception and Error Reports*	Section 5
CBP Directive No. 5610-004B, Budget Clearing Account (BCA) and Suspense Item Report (ACSR-CL-800) Attachment	Part 8
Code of Federal Regulations, Title 19	§111.25, §113.13, §113.15, §113.65, §163.4, §191.15, §191.38, §191.51, & §191.92
GAO *Standards for Internal Control in the Federal Government* (GAO-14-704G)	Principle 10, 11, 12, & 16
Statement of Federal Financial Accounting Standards 7: *Accounting for Revenue and Other Financial Sources and Concepts for Reconciling Budgetary and Financial Accounting*	Paragraph 53

II-F Grants Management	
FEMA CF-FM, *Accounting Accrual - Grants - PARS*, Number 2600-001, Version 9.0	Step 7, Appendix B
FEMA CF-FM-AA, *Disaster Grants and FEMA/State Agreement Closeouts*, Number 2600-017, Version 4.0	Chapter 4
FEMA *Single Audits of Federal Financial Assistance*, FD 077-2 Revision Number: 01	Section A, Section D
GAO *Standards for Internal Control in the Federal Government* (GAO-14-704G)	Section 1 & 2 Principle 10, 11, & 12
OMB, 2 CFR Chapter I, and Chapter II, Parts 200, 215, 220, 225, and 230, *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards*	§ 200.501, § 200.513, & § 200.521

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

Homeland Security

November 14, 2017

MEMORANDUM FOR: John Roth
Inspector General

FROM: Stacy Marcott
Chief Financial Officer (Acting)

SUBJECT: Fiscal Year 2017 Financial and Internal Controls Audit

Thank you for your audit report on the Department's financial statements and internal controls over financial reporting for fiscal years (FY) 2016 and 2017. We agree with the Independent Public Accountant's conclusions. We are proud of our fifth consecutive unmodified financial statement audit opinion.

The Department has made strides to mature our organization from both an audit remediation and internal control perspective. Our highest priority is supporting the critical mission of DHS with reliable financial information, and we have implemented robust oversight to ensure the integration of controls and standard business processes across the Department. Our leadership is also focused on working with the few remaining DHS components experiencing enterprise level control challenges in terms of staffing, training or coordination.

The audit report notes that the Department's long-standing material weakness over Property, Plant, and Equipment has been reduced in severity and is now considered a significant deficiency. This improvement is the result of substantial progress across the Department, most notably at the United States Coast Guard. Over the years, the Department has demonstrated the ability to resolve material weaknesses, from 10 in 2006 to two in FY 2017. We will continue our efforts to remediate control weaknesses in FY 2018, moving forward on the path to an unmodified opinion on our internal control over financial reporting.

I look forward to working collaboratively with the Office of Inspector General and the Independent Public Accountant to further strengthen DHS financial management and internal control.

Appendix B
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
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