OFFICE OF INSPECTOR GENERAL

Independent Auditors' Report on DHS' FY 2018 Financial Statements and Internal Control over Financial Reporting

Homeland Security

November 15, 2018

OIG-19-04

DHS OIG HIGHLIGHTS

Independent Auditors' Report on DHS' FY 2018 Financial Statements and Internal Control over Financial Reporting

November 15, 2018

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 61 recommendations that, when implemented, would 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, 2018.

KPMG issued an adverse opinion on DHS' internal control over financial reporting of its financial statements as of September 30, 2018. 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 laws and regulations:

Significant Deficiencies

1. Information Technology Controls and Financial Systems
2. Financial Reporting
3. Entity-Level Controls
4. Property, Plant, and Equipment
5. Custodial Activities: Entry Process, Refunds and Drawbacks, and Seized Property
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. *Antideficiency Act*
4. *Federal Financial Management Improvement Act of 1996*

Management's Response

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

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

November 15, 2018

MEMORANDUM FOR: The Honorable Kirstjen M. Nielsen
Secretary
Department of Homeland Security

FROM: John V. Kelly
Senior Official Performing the
Duties of Inspector General

SUBJECT: *Independent Auditors' Report on DHS' FY 2018 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) 2018 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 2018 *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 2018 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 reported the following significant deficiencies in internal control in six areas, of which two are considered material weaknesses, and four instances of noncompliance with laws and regulations:

Significant Deficiencies Considered To Be Material Weaknesses

- Information Technology Controls and Financial Systems
- Financial Reporting

Other Significant Deficiencies

- Entity-Level Controls
- Property, Plant, and Equipment

- Custodial Activities: Entry Process, Refunds and Drawbacks, and Seized Property
- 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 control 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 15, 2018, 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 Sondra McCauley, Assistant Inspector General for Audits at (202) 981-6000; 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), which comprise the consolidated balance sheets as of September 30, 2018 and 2017, 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, 2018, 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 the Financial Statements and 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 DHS'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. 19-01, *Audit Requirements for Federal Financial Statements*. Those standards and OMB Bulletin No. 19-01 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. We have identified material weaknesses in the following two areas:

A. Information Technology Controls and Financial Systems
B. Financial Reporting

These material weaknesses are described in Exhibit I and included in the *Secretary's Assurance Statement.* 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, 2018 and 2017, 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, 2018, 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 2018 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, DHS had intragovernmental debt of approximately $21 billion, and $30 billion used to finance the *National Flood Insurance Program* (NFIP) as of September 30, 2018 and 2017, respectively. Due to the subsidized nature of the NFIP, DHS has determined that future insurance premiums, and other anticipated sources of revenue, may not be sufficient to repay this debt. As discussed in Note 15 of the consolidated financial statements, on October 26, 2017, Congress enacted the *Additional Supplemental Appropriations for Disaster Relief Requirements Act of 2017*. This act cancelled $16 billion of DHS's debt that was 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*.

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.

KPMG

Other Reporting Required by Government Auditing Standards

Internal Control Over Financial Reporting

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. 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, Refunds and Drawbacks, and Seized Property
F. Grants Management

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 fiscal year 2018 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. 19-01, 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 fiscal year 2018 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.

DHS's Responses to Findings

DHS's responses to findings identified in our audit are described in Appendix A. DHS's responses were not subjected to the auditing procedures applied in the audit of the fiscal year 2018 consolidated financial statements and, accordingly, we express no opinion on these responses.

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 15, 2018

The weaknesses in internal control and findings related to compliance with certain provisions of laws, regulations, contracts, and grant agreements, presented herein, were identified during our audit of the U.S. Department of Homeland Security's (DHS) financial statements and internal control over financial reporting as of and for the year ended September 30, 2018. All Components of DHS, as defined in Note 1A – *Reporting Entity* to the financial statements, were considered in the scope of our audit of DHS' financial statements and internal control over financial reporting. The determination of which control deficiencies rise to the level of a material weakness or 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, 2018.

Our 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. We have reported material weaknesses within the following two areas:

A. Information Technology Controls and Financial Systems
B. Financial Reporting

Exhibit II Significant Deficiencies. A significant deficiency in internal control over financial reporting is less severe than a material weakness, yet important enough to merit attention of DHS management and others in positions of DHS oversight. We have reported four significant deficiencies in the following areas:

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

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. 19-01, *Audit Requirements for Federal Financial Statements*. We have reported four instances of noncompliance:

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*

Criteria We audited DHS's internal control over financial reporting based on the criteria established by *Standards for Internal Control in the Federal Government* issued by the Comptroller General of the United States (Green Book).

I-A Information Technology Controls and Financial Systems

Background: Information technology (IT) controls are a critical subset of an entity's internal control. Green Book principle 11 indicates that management should design the entity's information system and related control activities to achieve objectives and respond to risk. There are two main types of IT controls: IT general controls (ITGCs) and application controls. ITGCs 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, operating system, database, and application level, and include controls over security management, access control, configuration management, segregation of duties, and contingency planning. Effective ITGCs 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 complete and accurate processing of data.

During our fiscal year (FY) 2018 assessment of ITGCs, we noted DHS continued to design and implement controls to remediate IT findings related to user recertifications and password settings we reported in FY 2017, however, we identified new findings related to the operating effectiveness of controls in FY 2018. Additionally, management did not take sufficient corrective action to address deficiencies in multiple information systems that we identified and reported to management as a material weakness for several years.

As DHS moves forward with its financial systems modernization efforts, it is critical that DHS's modernization plans capitalize on the results from prior modernization efforts, as well as correct for current internal and external findings.

Conditions Related to ITGCs: The control deficiencies in ITGCs represent an elevated risk of material misstatement as DHS has an absence of sufficient manual, compensating controls in its process areas to fully mitigate these ITGC deficiencies. Deficiencies indicated in this Exhibit are representative of ITGC deficiencies identified at various Components across DHS. We identified the following:

Access Controls/Segregation of Duties:

DHS did not:

- adequately and consistently design, implement, and operate effective controls over initial authorization and periodic recertification of application, database, and operating system user, service, privileged, 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, including 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, including defining events that should be logged;
- 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; and
- maintain appropriate segregation of duties between development and production environments.

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 identified access control failures across multiple Components. In addition, DHS Components use other service providers to provide infrastructure support for various IT systems. We tested controls operated by these service providers and noted inconsistent oversight of the service provider and additional access control failures.

Configuration Management:

DHS did not consistently or completely:

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

In addition, we identified Security Management and Contingency Planning ITGC deficiencies.

Conditions Related to Financial Systems: During our audit, we also evaluated and considered the impact of financial system functionality on financial reporting. Historically, we noted that limitations in DHS'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 the *Federal Financial Management Improvement Act of 1996 (*FFMIA) and OMB Circular No. A-123, Appendix D, *Compliance with the Federal Financial Management Improvement Act of 1996*. Several DHS Components implemented and supported ITGCs and financial process areas with manual processes, decentralized systems or records management processes, or utilities with limited automated capabilities. These functionality limitations caused a greater 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 DHS. For example, system configurations and posting logic deficiencies limited the effectiveness of controls to accurately record certain activity at the transaction level. 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 DHS. 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; complex, highly interrelated yet decentralized nature of systems and system components; failure of communication between offices in the same organization regarding ITGC ownership; absence of continual self-review and risk assessments performed over ITGCs; 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.

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 DHS's ability to process, store, and report financial data in a manner that ensures accuracy, confidentiality, integrity, and availability. The aggregate impact of the ITGC deficiencies result in a 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 ITGCs are rendered ineffective. Ineffective process level application controls, in turn, create a need for mitigating controls which were often not present or not 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 absence of manual mitigating controls, which contributed to the findings reported in Exhibits I, II, and III. Furthermore, due to these

ITGC deficiencies, we deemed certain key manual controls throughout DHS ineffective, as they are dependent upon application controls to ensure the information produced from systems is complete and accurate.

Recommendations: We recommend that:

1. the DHS 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, make the necessary improvements to DHS's ITGC and application controls. Specific, more detailed recommendations were provided in individual limited distribution Notice of Findings and Recommendations to DHS and Component management;
2. DHS consider the identified system deficiencies and prior system implementation challenges to ensure that improvements in ITGC and application controls are designed, implemented, and sustained in new systems;
3. DHS establish an effective internal control process to ensure that financial accounts and transactions that are susceptible to error due to IT systems functionality issues and inability to rely on application controls supported by deficient ITGCs are compensated for with manual controls until system deficiencies are remediated; and
4. DHS ensure 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.

I-B Financial Reporting

Background: 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 the applicable financial reporting framework.

In FY 2018, DHS continued to implement corrective action plans and made progress in certain areas. However, the United States Secret Service (USSS) continues to have challenges due to the financial system upgrade and business process changes. We identified new deficiencies, some of which are directly related to the system transformation USSS completed in FY 2018. In contrast, United States Coast Guard (USCG) management sustained the progress made in FY 2017 and continued to demonstrate greater understanding of the actuarial pension and healthcare valuation processes, including assumptions and sources of data used in the valuations. However, as described below, USCG management should continue to refine the management review controls over actuarial liabilities. We also identified a new deficiency related to a specific accounting transaction at the Federal Emergency Management Agency (FEMA).

Conditions and causes across DHS:

- DHS did not demonstrate a commitment to recruiting, developing or retaining competent individuals as required by Green Book principle 4.
- DHS did not identify, analyze, and respond to risks related to financial reporting as required by Green Book principle 7.
- DHS did not remediate identified internal control deficiencies as required by Green Book principle 17.
- DHS has not established robust monitoring and testing of ITGCs that is necessary to identify weaknesses, nor has it assessed the resulting risks created by IT deficiencies. Therefore, DHS lacked sufficient manual process level controls to fully mitigate the weaknesses caused by ITGC deficiencies.
- DHS does not have sufficient monitoring controls to ensure that Components have sufficient controls for the consistent application of allocation methodologies for the Statement of Net Cost.

- DHS 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. Personnel tasked with evaluating the roles 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.

Effect: The lack of compensating controls for IT deficiencies results in DHS'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*. Several Components failed to adequately review their Statement of Net Cost footnote templates to ensure they were completed accurately during the year. This resulted in auditor-identified errors in the allocation percentages used across DHS goals.

Conditions and causes related to the review and approval of journal entries:

- USSS did not design and implement effective controls over journal entries. Due to gaps in the number of financial management personnel with the appropriate skills, and in well-defined policies and procedures, USSS personnel did not have sufficient knowledge to properly perform the review and approval of journal entries. USSS staffing challenges are compounded by stringent security clearance processes, which impair management's ability to quickly hire and on-board qualified personnel. In addition, USSS did not provide adequate training and coordination for recording on-top adjustments. Specifically:
  - journal entries were directly entered into the 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;
  - journal entries were directly entered into the financial system, for which review and approval was not evidenced;
  - entries related to the pension liability and expense were not recorded for the proper amounts or to the correct U.S. Standard General Ledger (USSGL) accounts; and
  - the general ledger system allowed certain users to enter transactions without following the appropriate posting logic and lines of accounting.
- USCG did not design and implement controls related to the review and approval of journal entries. The USCG's three legacy general ledger systems, developed over a decade ago, have functional limitations and necessitate large manual adjusting entries to compensate for the inability to record transactions correctly upon initiation. The magnitude of these entries inhibit management from performing adequate reviews of activity for reasonableness and alignment with the current year's business events. These system functionality limitations also hinder USCG's ability to ensure accuracy of certain beginning balances and year-end close-out activities at a transaction level. Specifically, there were not effective controls:
  - over the review of manual adjusting journal entries to prevent and/or detect and correct financial reporting errors and to ensure their alignment with actual current year business events; and
  - to ensure the accuracy of certain beginning balance and year-end close-out activities, at the transaction level, in its three general ledgers due to manual adjusting entries for all activity only being recorded to one general ledger.

Effect: The failure to adequately design and implement internal controls over journal entries increases the risk that errors can occur without being prevented and detected.

Conditions and causes related to technical accounting determinations:

Congress passed the Additional Supplemental Appropriations for Disaster Relief Requirements Act of 2017 (Pub. L. 115-72) on October 26, 2017, which provided debt relief and additional borrowing authority for the National Flood Insurance Program (NFIP) by cancelling $16 billion of the NFIP's debt to the U.S. Department of the Treasury. DHS and FEMA did not design and implement effective controls to properly account for the proprietary impact of Pub. L. 115-72. FEMA did not properly apply the generally accepted accounting principles (GAAP) hierarchy to ensure the transaction was accounted for in accordance with Statement of Federal Financial Accounting Standards 7 No: *Accounting for Revenue and Other Financing Sources and Concepts for Reconciling Budgetary and Financial Accounting*. In addition, DHS failed to properly monitor FEMA's controls to ensure that a non-routine and material transaction, which impacted the DHS consolidated financial statements, was properly recorded.

Effect: This resulted in an auditor-identified $16 billion adjustment that DHS corrected to properly present the Statement of Changes in Net Position.

Conditions and causes related to actuarially derived 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 overreliance on an external actuary. In addition, existing policies and procedures were not detailed enough to enable new employees to understand the design and implementation of the controls. USSS did not fully assess risk, design and implement sufficient controls, and document processes over its actuarial pension liability. Specifically, management did not implement:
  - controls at an appropriate level of precision for management review of assumptions used in the valuation of the liability;
  - policies and procedures to document its 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; and
  - controls to validate the completeness and accuracy of underlying data used in the valuation of the liability.
- USCG did not properly design, implement, or adequately document the operation of management review controls over actuarial liabilities. Specifically, management review controls lacked sufficient precision and timeliness to ensure the appropriateness of the assumptions used in the preparation of the actuarial liabilities.

Effect: This resulted in over $200 million in auditor-identified errors to the USSS actuarial pension liability and $105 million to the USCG actuarial pension liability.

Other financial reporting-related conditions:

- USSS did not effectively plan and train for new processes required as a result of the system transformation. USSS did not establish processes or controls to verify that financial transactions received during the system transformation were completely and accurately tracked, monitored, and entered into the financial system on a timely basis.
- USSS did not have properly designed and implemented controls over the preparation and review of accounting checklists.
- USSS did not effectively design its controls over the monitoring of obligated balances, including an inability to readily generate an open obligations report.

- Financial system functionality issues hindered USCG's ability to ensure that transactions were recorded and assigned to the correct trading partner at the time of the business event. USCG did not have properly designed and implemented controls to reconcile intra-governmental activities and balances and to ensure that transactions were recorded and assigned to the correct trading partner at the time of the business event.

Effect: The aggregate result of the financial reporting deficiencies is a risk that a misstatement will not be prevented or detected and corrected in a timely manner.

Recommendations: We recommend that:

DHS:

5. fill needs for technical and resource support personnel to remediate control deficiencies or prevent deterioration of the internal control system;
6. assess training needs for personnel and align skills with roles and responsibilities, and ensure 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;
7. define succession and contingency plans for key roles involved in internal control over financial reporting to mitigate risks due to employee turnover;
8. improve the process for identification, analysis, and response to risks related to financial reporting;
9. strengthen monitoring controls over remediating internal control deficiencies;
10. develop continuous monitoring and testing of ITGCs to identify weaknesses, assess the resulting risks created by any identified IT deficiencies, and respond to those risks by implementing compensating controls;
11. develop and implement monitoring controls to ensure Components properly apply allocation methodologies for the Statement of Net Cost;
12. 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; and
13. establish a process to ensure accounting for non-routine material transactions impacting the financial statements is appropriate.

USSS:

14. develop and implement policies and procedures over the review of journal entries;
15. establish new, or improve existing, policies, procedures, and related internal controls over the valuation of its pension liability to ensure:
    a. adequate understanding of the pension estimate;
    b. oversight of assumptions used in significant estimates is maintained and the validity of those assumptions is routinely evaluated;
    c. the annual pension checklist developed by USSS is completed; and
    d. the underlying census data is reviewed at least annually;
16. provide sufficient training to personnel responsible for accounting related activities, including the processes resulting from the system transformation and the monitoring of obligations; and
17. design and implement controls over the preparation and review of accounting checklists.

USCG:

18. improve and reinforce existing policies, procedures, and related internal controls to ensure that:
    a. journal entries and manual adjusting entries are adequately researched, supported, and reviewed before and after recording in the general ledger;
    b. manual adjusting entries are recorded at the transaction level in the correct underlying general ledger systems in order to generate accurate beginning balances in each system;
    c. design and implement control procedures to ensure that assumptions are sufficiently reviewed on a timely basis with an appropriate level of precision, and that the results of these reviews are properly documented; and
    d. transactions are recorded to the accurate trading partner upon initiation; all intra-governmental balances are reconciled with trading partners; and differences are resolved in a timely manner.

FEMA:

19. develop specific controls over material accounting transactions that are not part of FEMA's routine business operations.

II-C Entity-Level Controls

Background: Entity-level controls are defined by the *Standards for Internal Control in the Federal Government* issued by the Comptroller General of the United States (Green Book) as controls that have an effect on an entity's internal control system and may pertain to multiple components of internal control. Entity-level controls may include controls related to the entity's risk assessment process, control environment, service organizations, management override and monitoring. These controls must be effectively designed, implemented, and operating effectively in an integrated manner to create and sustain an organizational structure that is conducive to reliable financial reporting.

Conditions, Cause/Effect, and Recommendations: During our audit, we identified certain deficiencies in entity-level controls. Certain of these deficiencies are included in the conditions and causes in Exhibit I. Other deficiencies are included below. The resulting recommendations include improvements needed in management's control environment, risk assessment process, communication practices throughout DHS, and its monitoring activities. Improvements in these areas are necessary 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: DHS 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 DHS Management-level leadership is required to address the following areas of the control environment at certain Components:

20. ensure significant accounting policies and standard operating procedures are formally documented, complete, updated, and revised timely;
21. define roles and responsibilities of program and field personnel that provide key financial information, and ensure those personnel understand and comply with policies; and
22. establish a structure with central ownership and oversight for internal controls where responsibilities have been delegated to discrete units.

Risk Assessments: DHS 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 DHS 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:

23. procedures to expand fraud risk assessments to include processes with higher risk and a known deficiency in control design, implementation, and effectiveness throughout DHS;
24. planned changes that could impact the internal control system, such as financial system transitions and implementation of new tools; and
25. 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.

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

26. coordination between headquarters and Components with resource constraints to respond to financial accounting and reporting risks and control deficiencies;

27. 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;
28. individuals within the financial reporting, accounting and budget departments identify and use quality information for financial reporting;
29. communication of the roles and responsibilities of program and field personnel that provide key financial information, and that those personnel understand and comply with policies; and
30. 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, DHS continued to make progress in identifying and remediating control deficiencies in certain areas. However, DHS 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:

31. design continuous monitoring controls to ensure personnel with internal control oversight responsibilities adequately examine transactions with higher risk of error;
32. seek opportunities to implement more reliable controls earlier in the process to prevent errors at the transaction source; and
33. enhance internal testing of both IT and financial 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 2018, USSS continued to experience significant issues in its design and implementation of controls over property, plant, and equipment financial reporting. USSS has taken initial steps to account for its property through a physical count of property, plant and equipment.

The USCG sustained the progress they had made in FY 2017; however, some control deficiencies related to property, plant, and equipment persisted.

The National Protection and Programs Directorate (NPPD) has a continuing issue with the review of expenses to ensure that they are capitalized timely.

Conditions:

USSS did not:

- implement established inventory policies and control procedures to ensure the completeness, existence, and accuracy of property, plant and equipment;

- design and implement sufficient controls to reconcile its property, plant, and equipment detailed sub-ledger to the general ledger and appropriately track asset activity at a transaction level, and ensure the timely recording of asset additions, deletions, or other adjustments to property, plant, and equipment;
- design and implement sufficient controls to appropriately report the asset placed in service date, maintain support for the date used, and analyze and disaggregate the useful lives among types of property, plant and equipment; and
- design and implement controls to determine and review the capitalization thresholds established or identify instances of and criteria for property, plant, and equipment asset impairment.

USCG did not:

- design and implement sufficient controls over the physical count of real property assets to ensure assets are appropriately and timely inventoried to verify their continued existence as recorded in the general ledger; and
- have controls that were operating effectively over the timely recording of fixed asset addition and retirement activity in the general ledger.

NPPD did not:

- implement control activities to identify contracts and expenditures that by their nature can be capitalized, ensure expenditures are appropriately capitalized in a timely manner, and consistently implement manual compensating controls.

Cause: USSS performed an inadequate assessment of risks and failed to implement controls related to the capital property processes, including the proper integration between the sub-ledger and general ledger. USSS also had inappropriate resources to monitor and oversee the reporting and recording of capital property. Furthermore, insufficient communication existed among USSS internal groups to ensure proper accountability.

USCG management decided to focus FY 2018 remediation efforts on construction in progress internal control deficiencies rather than real property inventory and timely recording of asset activity deficiencies.

NPPD has not designed and implemented sufficient controls across the directorate to develop, document, implement, and perform robust internal control procedures.

Effect: USSS experienced significant difficulties in providing complete and accurate data to support operating controls and year-end property, plant, and equipment balances. The aggregate impact of the property, plant, and equipment deficiencies at USSS, USCG, and NPPD result in a risk that misstatements related to the completeness, existence, and valuation of property, plant, and equipment are not prevented, or detected and corrected in a timely manner. The potential errors identified for property, plant, and equipment were approximately $300 million.

Recommendations: We recommend that:

USSS:

34. design and implement controls and procedures to reconcile property, plant, and equipment between the sub-ledger and the general ledger and identify and investigate all significant differences;
35. 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;

36. design and implement sufficient controls to support and record the date property is placed in service and the useful lives of various types of personal property;
37. design and implement controls over the capitalization thresholds established for property, plant, and equipment;
38. design and implement controls and processes to identify instances and criteria for asset impairment;
39. establish new, or improve current, communication channels and standard operating procedures to ensure sufficient review of property, plant, and equipment activity and balances; and
40. attract and deploy additional skilled resources to support the control environment and provide the necessary financial reporting oversight.

USCG:

41. design and implement real property inventory controls to ensure the completeness and existence of all real property assets; and
42. reinforce controls over the timely recording of asset addition and retirement activity to ensure they operate effectively.

NPPD:

43. design and implement sufficient controls to properly record items that should be capitalized in a timely fashion.

II-E Custodial Activities: Entry Process, Refunds and Drawbacks, and Seized Property

Background: CBP comprises approximately 99% of DHS'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. CBP uses Centers of Excellence and Expertise (CEE) to align CBP's trade relationships with modern business practices. CBP pairs each CEE with specific industries (e.g., electronics) to create a uniformity of practices across ports of entry, and to facilitate the timely resolution of trade compliance issues for their specific industry.

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. TDTRs also include any fines, 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. The *Trade Facilitation and Trade Enforcement Act of 2015* (TFTEA) contains provisions for drawback modernization that simplify the rules for determining if exports are eligible for drawback refunds, expands the timeframe for drawback claims, and eliminates some of the documentation requirements. Refund claims are a remittance, in whole or in part, of duties, taxes, or fees previously paid by an importer. Refund claims typically occur when previous payments are identified as having been made at the incorrect rate due to free trade programs (i.e., North American Free Trade Agreement) or errors in the classification of goods imported into the United States.

Many of the conditions cited below have existed for several years. As of February 24, 2018, all refund and drawback requests are processed in the automated commercial environment (ACE). The transition from the legacy system allows for the implementation of additional automated controls. However, until the finalization of the TFTEA legislation and submission of claims under related provisions, the drawback conditions below will continue to exist.

CBP seizes various items including prohibited drugs and counterfeit goods. Although CBP does not have law enforcement authority to prosecute cases, seizures are maintained for evidence. CBP is also the primary custodian for U.S. Immigration and Customs Enforcement (ICE) seizures. CBP relies on ICE to enter case information including weights and measures into the seized property system for tracking purposes.

Conditions: We identified the following internal control deficiencies related to custodial activities at CBP and ICE 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 entry edit and exception reports. Specifically, items may be included on the report for a given CEE, though not processed by that CEE, and therefore are not subject to the same level of review.
- CBP did not fully establish controls over the inputs to the TDTR estimate. There were instances where rates used in the Supplemental Duties Bills estimation model were calculated incorrectly.

Related to Refunds and Drawbacks:

- The current drawbacks IT system at CBP 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 claims were based. Further, the system had not been configured to restrict drawback claims to the statutory limits, in accordance with regulations for applicable drawback claims.
- Documentation retention periods were not appropriate to ensure that importers maintained support for drawback transactions for the full claim time-period. CBP did not always maintain support for importers qualifying for accelerated filer status at one port.
- Controls over refund disbursements were not operating effectively. Refund disbursements were made without proper review and approval. In addition, controls over the calculation of interest were not operating effectively to prevent the miscalculation of interest paid for certain refunds.

Related to Seized Property:

- The design of CBP's monthly review control over seized property was inadequate, as it did not identify unusual weight and measure variances needing further investigation.
- CBP had not designed and implemented adequate controls to verify that the data used to produce the Seized and Forfeited Property Footnote was complete and accurate.
- CBP lacked sufficient controls over the system configuration used to generate seized and forfeited property reports to ensure all activity, including turnover seizures, was captured and reported.
- Processes were not implemented to ensure seized asset transactions were properly and timely recorded in the seized assets tracking system at CBP and ICE.

Cause/Effect: Policies and procedures over the review of entry edit, and exception reports were not sufficient to ensure personnel performed the controls consistently at all ports and CEE during FY 2018. In addition, existing policies and procedures do not require timely coordination with all applicable parties. Failure to adhere to existing policies and procedures consistently 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 Activity. Inadequate controls could result in CBP's failure to identify amounts that are due to the Treasury General Fund.

Failure to fully establish and define control activities related to the entry process could lead to potential misstatements of net TDTR on the DHS Balance Sheet and total cash collections on the Statement of Custodial Activity.

IT system functionality and outdated IT systems contribute to the weaknesses identified above. Refer to Comment **I-A**, *Information Technology Controls and Financial Systems*. The current refunds and drawbacks IT system does not prevent the overpayment of legacy drawback claims. Once the TFTEA drawback provisions are finalized the system configurations will be updated to ensure proper processing of claims filed under TFTEA. CBP does not currently have sufficient resources to effectively perform compensating manual controls over drawback claims. TFTEA changed the statutes that govern the drawback process and further reduced the need for manual controls. The length of the drawback claim lifecycle often extends beyond the documentation retention period, which is set by statute. Until effective automated or compensating 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 for years, it will take several years for claims existing prior to the implementation of TFTEA to be completed. In addition, CBP did not adequately research and determine the root cause of incorrect system interest calculations.

CBP is responsible for reporting seized and forfeited property that is in its custody. CBP relies on other entities to enter seizures into the seized property system, but as the custodian, CBP did not recognize their responsibility to design an effective review process over the input, extraction, or reporting of seized and forfeited property activity. In addition, ICE did not properly train employees on how to use the seized property system. The errors in the seized property data resulted in overstatements of various weights and measures that required correction in the FY 2018 consolidated financial statements.

Recommendations: We recommend that CBP:

Related to the Entry Process:

44. update and redistribute guidance to appropriate personnel regarding the relevant CBP directives to ensure consistent performance of controls across all locations;
45. provide training to all personnel on new policies to ensure consistent implementation at decentralized locations;

Related to Refunds and Drawbacks:

46. continue implementing requirements of TFTEA, which will take full effect beginning on February 24, 2019;
47. continue to enhance 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;
48. revise current policies and procedures to ensure appropriate personnel review and approve all refunds prior to disbursement;

49. revise policies and procedures to ensure effective review of the interest calculation for refund disbursements;
50. implement policies and procedures to ensure supporting documentation for accelerated filer status is maintained;

Related to Seized Property:

51. improve the design of existing review controls over monthly seized property reports;
52. redesign and implement controls over the completeness and accuracy of the data used for reporting purposes; and
53. redesign and implement controls, in coordination with ICE, to validate that weights and measures entered into the seized property system are complete and accurate.

II-F Grants Management

Background: FEMA is the primary grantor within DHS, and manages multiple Federal disaster and non-disaster grant programs. In FY 2018, FEMA began implementation of the process to standardize all grant management activities. This included coordination among the grant regional offices and headquarters as well as among the various grant programs. Although not fully implemented in FY 2018, FEMA has established policies and procedures that have been partially executed in FY 2018.

Conditions: The internal control deficiencies related to grants management were reported in the prior year and persisted in FY 2018. 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;
- demonstrate effective monitoring of grantees, reconcile grantee quarterly financial reports to FEMA's systems consistently and effectively, and timely closeout of FEMA grants; and
- issue Management Decision Letters timely for single audit reports available in the Federal Audit Clearinghouse.

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 Title 2 of the Code of Federal Regulations (CFR), Part 200 - *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards* (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 grant systems to FEMA's general ledger system, and to track grants eligible for closeout. Refer to Comment **I-A**, *Information Technology Controls and Financial Systems*. Historically, responsibilities surrounding grants management have been assigned to discrete units within the organization, and there was no overall central oversight to ensure the delegated responsibilities were being effectively carried out for all grants. In FY 2018, FEMA implemented grant management guidance with policies and procedures applicable to the discrete units within FEMA. However, the internal controls based on these policies and procedures were not implemented for the entire fiscal year. 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 failure to implement standardized internal controls within FEMA for all of FY 2018 caused difficulty assembling a comprehensive status of cash on hand at grantees and the status of grants eligible for closeout, thereby creating risk of excessive cash on hand at grantees and untimely closure of grants.

Recommendations: We recommend that FEMA:

54. implement a continuous quality assurance and grants monitoring process, including review of corrective actions resulting from procedures over obtaining, timely reviewing, and reconciling required quarterly grantee reports and procedures to create and track comprehensive lists of FEMA grants eligible for closeout; and
55. 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.

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 FMFIA. DHS has implemented a multi-year plan to achieve full assurance on internal control. However, the DHS *Secretary's Assurance Statement*, dated November 15, 2018, as presented in *Management's Discussion and Analysis* of DHS's FY 2018 *Agency Financial Report* (AFR), 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, 2018. Management's findings were similar to the control deficiencies we have described in Exhibits I and II. However, continuous monitoring and testing of both IT and financial controls was not performed for all significant areas.

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

Recommendation: We recommend that DHS:

56. 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 for FY 2019; and
57. conduct complete risk assessments to identify significant risk areas and continuously monitor and test IT and financial controls within those areas.

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

FEMA is the primary grantor within DHS, managing multiple Federal disaster and non-disaster grant programs. The *Single Audit Act Amendments of 1996*, as implemented by the 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 of the Super Circular in FY 2018. We noted that FEMA implemented some standardized grants management processes during the year, including new monitoring policies. However, FEMA did not review all grantee single audit reports in a timely manner. The failure to implement controls over grants management prevents FEMA from being able to monitor its grantees' compliance with applicable laws and regulations effectively.

Recommendation: We recommend that FEMA:

58. 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 ongoing within DHS have identified, 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. In FY 2017, the package to notify the President, Congress, and the U.S. Government Accountability Office (GAO) of the violation was signed by the DHS Secretary. OMB cleared the package in FY 2018 and the DHS Office of Legislative Affairs is working with OMB on next steps to deliver the package.
- In FY 2016, 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 2017, 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 pending OMB clearance.
- In FY 2018, DHS finalized its investigation related to 42 contract violations (11 with CBP, four with FEMA, three with the Federal Law Enforcement Training Center, two with ICE, nine with the Management Directorate, 12 with USCG, and one with USSS) and 104 Other Transaction Agreements with the Transportation Security Administration in excess of $1 million awarded from FY 2010 to FY 2016 without the appropriate Congressional notification. The package to notify the President, Congress, and GAO of the violation is pending OMB clearance.
- CBP is investigating a potential ADA violation related to overtime in excess of the annual cap established in the FY 2015 appropriations acts. DHS is waiting on the decision to a litigation case before finalizing the report.
- CBP is investigating a potential ADA violation related to the obligation of funds on uniform contracts from FY 2005 to FY 2011 with an open-ended buyout clause.
- In FY 2018, USSS completed an investigation of a potential ADA violation related to accepting voluntary services in FY 2014. The preliminary investigation report is pending review from legal counsel.
- USCG is investigating a potential ADA violation related to obligating funds in advance of appropriation during a Government shutdown in FY 2018.
- USCG is investigating a potential ADA violation related to potentially obligating funds in FY 2018 on an anchor chain sourced from China in violation of the Buy American Act and the appropriation.
- USCG is investigating a potential ADA violation in FY 2017 and FY 2018 related to obligating funds from an expired FY 2016 appropriation.
- USCG is investigating a potential ADA violation related to 20 leases signed with open-ended indemnification clauses, unlimited liability, and/or indeterminate amounts from FY 1972 to FY 2015.
- FEMA investigated a potential ADA violation related to obligating funds in FY 2017 under the Federal Assistance appropriation instead of the Procurement Construction & Improvement appropriation and concluded it was not an ADA violation.
- The DHS Financial Operations Division (OFO) is investigating a potential ADA violation related to obligating funds in the Working Capital Fund in excess of the Fund Balance with Treasury, creating a negative balance.

Recommendation: We recommend that DHS:

59. reinforce existing policies and procedures through training to strengthen the implementation and effectiveness of preventative controls; and

60. 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 15, 2018, that DHS's financial management systems do not substantially conform to government-wide requirements mandated by FFMIA. DHS's remedial actions and related timeframes are also presented in the FY 2018 AFR.

An element within FFMIA, Federal system requirements, entails 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 Systems*, which impact DHS's ability to fully comply with FISMA.

Recommendation: We recommend that DHS:

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

Appendix A
Management Comments to the Draft Report

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

Homeland Security

NOV 14 2018

MEMORANDUM FOR: John V. Kelly
Senior Official Performing the Duties of the Inspector General

FROM: Stacy Marcott
Acting Chief Financial Officer

SUBJECT: Fiscal Year 2018 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) 2018 and 2017. We agree with the Independent Public Accountant's conclusions. We are pleased to have earned an unmodified financial statement audit opinion for the sixth consecutive year.

Despite the complexities of disparate financial systems and associated business processes, management continues to make and sustain progress at many of our large Components such as the United States Coast Guard, as noted in your report. The report also highlights significant financial reporting challenges at the United States Secret Service (USSS), many of which are related to a recent system upgrade. Although USSS accounts for less than 2% of total assets and budgetary resources, we take the report's findings very seriously and are committed to assigning the necessary resources to ensure remediation of these deficiencies.

In regard to information technology controls, we have prioritized and are addressing the most significant internal control issues across the DHS financial systems portfolio. These efforts span multiple years and are tightly monitored, yielding results now, with a clear path to future internal control maturity. We are confident that with continued commitment to and investment in our DHS financial management community, our steady progress will continue in FY 2019.

I look forward to working collaboratively with the Office of Inspector General and the Independent Public Accountant in the years ahead 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