OFFICE OF INSPECTOR GENERAL

Summary Report: Persistent Data Issues Hinder DHS Mission, Programs, and Operations

Homeland Security

May 24, 2021
OIG-21-37

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

May 24, 2021

MEMORANDUM FOR: Eric Hysen
Chief Information Officer
Department of Homeland Security

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

JOSEPH V CUFFARI
Digitally signed by JOSEPH V CUFFARI
Date: 2021.05.21 14:22:12 -04'00'

SUBJECT: *Summary Report: Persistent Data Issues Hinder DHS Mission, Programs, and Operations*

Attached for your action is our final *Summary Report: Persistent Data Issues Hinder DHS Mission, Programs, and Operations.* We incorporated the formal comments from the Departmental GAO-OIG Liaison Office in the final report. We made no recommendations in this summary report.

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

Please call me with any questions, or your staff may contact Thomas Kait, Acting Deputy Inspector General for Audits, at (202) 981-6000.

Attachment

DHS OIG HIGHLIGHTS

Summary Report: Persistent Data Issues Hinder DHS Mission, Programs, and Operations

May 24, 2021

Why We Did This Review

Federal agencies create and collect large amounts of data as they carry out their missions. Improving the quality, security, and transparency of Federal data has been a priority of the President, Congress, and Department of Homeland Security in recent years. We conducted this review of DHS Office of Inspector General reports issued from fiscal years 2017 to 2019 to identify frequently reported findings and quantify persistent and systemic data issues that hinder DHS' ability to accomplish its mission operations.

What We Recommend

We made no recommendations in this summary report.

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

Significant challenges hinder the Department of Homeland Security's day-to-day use of some of the Nation's largest and most diverse databases to support its vast mission operations. DHS needs to improve the collection and management of data across its multiple components to better serve and safeguard the public. The data access, availability, accuracy, completeness, and relevance issues we identified presented numerous obstacles for DHS personnel who did not have essential information they needed for decision making or to effectively and efficiently carry out day-to-day mission operations.

We attributed the systemic data issues identified to widespread deficiencies that can be grouped into five categories: security and technical controls, program and operational oversight, guidelines and processes, system design and functionality, and training and resources.

DHS has improved its information security program and developed various plans and strategies to improve the quality and management of its data. Corrective actions in response to recommendations made in our prior reports are also good steps forward. However, follow-through and continued improvement will be essential to address the internal control issues underlying the data deficiencies we highlighted. Only then can the Department be assured it captures reliable and accurate data to accomplish its mission responsibilities.

DHS Response

DHS provided written comments, which we have included in Appendix B.

Table of Contents

Background 1

Results of Review 3

Prevalent Data Issues Hinder DHS Programs and Mission Operations.... 3

Data Issues Were Attributed to Various Internal Control Deficiencies... 10

Opportunities for Improvement 15

DHS Comments and OIG Analysis... 17

Appendixes

Appendix A: Objective, Scope, and Methodology 20
Appendix B: DHS Comments to the Draft Report 21
Appendix C: Summary of Data Issues and Causes 24
Appendix D: FYs 2017–2019 DHS OIG Reports with Data Issues 25
Appendix E: Office of Audits Major Contributors to This Report 30
Appendix F: Report Distribution 31

Abbreviations

ATO	Authority to Operate
CBP	U.S. Customs and Border Protection
CLAIMS3	Computer Linked Application Information Management System
FDS	Federal Data Strategy
FEMA	Federal Emergency Management Agency
GAO	U.S. Government Accountability Office
ICE	U.S. Immigration and Customs Enforcement
IT	Information Technology
OHA	Office of Health Affairs
OIG	Office of Inspector General
OMB	Office of Management and Budget
R&D	Research and Development
S&T	Science and Technology Directorate
USCIS	U.S. Citizenship and Immigration Services

Background

Federal agencies create, collect, and manage large amounts of data to accomplish their various missions. Improving the quality, security, and transparency of Federal data has been a priority for the President, Congress, the Office of Management and Budget, and the Department of Homeland Security. During the past decade, Congress has passed several laws to improve the quality, security, management, and accessibility of Federal data. These laws include the *Digital Accountability and Transparency Act of 2014*, the *Federal Information Security Modernization Act of 2014*, the *Geospatial Data Act of 2018*, and the *Foundations for Evidence-Based Policymaking Act of 2018* (Evidence Act).

In March 2018, the President's Management Agenda established a cross-agency priority goal to create best practices for how agencies manage and use data. To promote the President's Management Agenda, the Office of Management and Budget established a multi-year Federal Data Strategy (FDS) in 2019. The FDS is a framework of operational principles and best practices intended to guide Federal data management and use. Through consistent data infrastructure and practices, the strategy will enable the Federal Government to fully leverage data as a strategic asset. The strategy describes a long-term vision, spanning 10 years, for how the Federal Government will accelerate the use of data to deliver on agency missions and serve the public while also protecting data security, privacy, and confidentiality.

As required by the *Evidence Act,* the Department designated its first Chief Data Officer in July 2019 with the authority and responsibility for data governance and lifecycle data management. The Office of the Chief Data Officer leads the Department's efforts to secure and manage data within the components and headquarters. One objective is to enhance mission effectiveness through quality data that is trusted, secure, and available.

Recognizing the importance of collecting, maintaining, and disseminating quality data, DHS developed an Enterprise Data Strategy for fiscal years 2017 to 2021 that provides a roadmap for effective data management, sharing, safeguarding, and integration department-wide. As described in the strategy, the Department's enterprise data vision is to provide every DHS component and mission operator access to accurate information to accomplish their mission and management activities. The Office of the Chief Data Officer collaborates with programs across DHS to implement the strategic objectives outlined in this strategy.

DHS currently has an inventory of more than 2,000 data sets in its enterprise architecture information repository. The responsibility for carrying out many DHS data management activities falls within the purview of the DHS Enterprise Data Management Office. This office has developed several guidelines and strategies to improve the Department's data management and quality. For example:

- The *2012 Enterprise Data Management Concept of Operations* provides guidance to DHS and its components on their management responsibilities for ensuring that DHS data is understandable, trusted, visible, accessible, and interoperable.

- The *2016 Data Stewardship Framework* describes roles and responsibilities and provides information about strategic, collaborative, and operational data stewardship within the broader context of Enterprise Data Management.

- The *2018 Data Dictionary Guidance* provides information about defining, managing, standardizing, controlling, and sharing data among and between individuals, organizations, Communities of Interest, and systems.

- The *Data Quality Guide*, *Data Modeling Guidelines*, and *Data Management Plan Guide*, all updated in 2019, provide data management and quality guidelines across the Department.

Adhering to such guidance should be key to improving data stewardship and use, and ensuring data quality across the Department. Equally important are recognizing existing deficiencies that impede DHS' progress leveraging data as a strategic asset and devising ways to overcome them. We conducted this review of our reports issued from FY 2017 to FY 2019 to assist the Department with identifying frequently reported findings and quantifying persistent and systemic data issues that hinder accomplishment of DHS mission operations.

Results of Review

Significant challenges hinder DHS' day-to-day use of some of the Nation's largest and most diverse databases to support its vast mission operations. DHS needs to improve the collection and management of data across its multiple components to better serve and safeguard the public. The data access, availability, accuracy, completeness, and relevance issues we identified presented numerous obstacles for DHS personnel, who did not have essential information they needed for decision making or to effectively and efficiently carry out day-to-day mission operations.

We attributed the systemic data issues identified to widespread deficiencies that can be grouped into five categories: security and technical controls, program and operational oversight, guidelines and processes, system design and functionality, and training and resources.

DHS has improved its information security program and developed various plans and strategies to improve the quality and management of its data. Corrective actions in response to recommendations made in our prior reports are also good steps forward. However, follow-through and continued improvement will be essential to address the internal control issues underlying the data deficiencies we highlighted. Only then can the Department be assured it captures reliable and accurate data to accomplish its mission responsibilities.

Prevalent Data Issues Hinder DHS Programs and Mission Operations

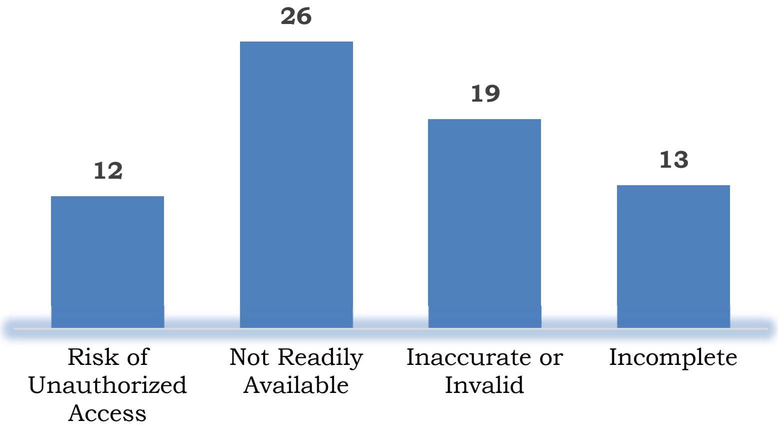
Managing and ensuring data quality is essential to DHS mission accomplishment, which entails making operational decisions that affect national security, lives, property, and quality of life. According to the U.S. Government Accountability Office's (GAO) *Standards of Internal Control in the Federal Government* (i.e., the Green Book),[1] management is responsible for obtaining relevant data from reliable sources in a timely manner based on the information requirements needed to achieve objectives and address risks. The Green Book also states that management is responsible for processing the obtained data into quality information to make informed decisions.

Our review of a total of 135 DHS Office of Inspector General (OIG) reports issued in fiscal years 2017 to 2019 revealed widespread data quality issues that negatively affected DHS programs and mission operations. Although these reports were based on a variety of audits and inspections of DHS programs and

[1] *Standards for Internal Control in the Federal Government,* GAO-14-704G, September 2014.

operations, we noted common data issues — pertaining to the integrity, reliability, and availability of DHS data — prevalent in more than a third of the reports.[2] Figure 1 summarizes these data challenges within DHS.

Figure 1. Data Issues Identified in DHS OIG Reports from FY 2017 to FY 2019



Source: DHS OIG analysis of FYs 2017–2019 DHS OIG reports

We identified a total of 70 instances that demonstrated data was not sufficiently confidential, available, complete, or accurate/valid to support DHS components in making operational decisions or effectively completing mission requirements. These data issues hindered a wide range of DHS mission responsibilities and operations, including law enforcement, cybersecurity, immigration, disaster assistance, acquisition, and financial reporting. We grouped these issues into four overarching categories: (1) data access, (2) data availability, (3) data accuracy, and (4) data completeness and relevance. Appendix C contains a summary of all data issues we identified.

Data Access: DHS Data Was at Risk of Unauthorized Access and Disclosure

A number of data access control deficiencies have persisted across the Department year after year. According to the Green Book, management has a responsibility to design and implement information system controls for appropriate access by internal and external sources to protect the confidentiality, integrity, and availability of data. Over the years, the Department has taken actions to implement our prior report recommendations, designed to improve financial management and information security controls. For example, our FY 2019 report on DHS' Information Security Program noted that the Department improved its level of maturity in two cybersecurity functions from FY 2017 and FY 2018 levels and has increased the number of

[2] In summary, 48 of the 135 reports we reviewed discussed prevalent data issues.

systems enrolled in the Ongoing Authorization Program from FY 2016 to FY 2018. As another example, U.S. Citizenship and Immigration Services (USCIS) implemented an electronic account request system, MyAccess, in response to our recommendation to institute a method to capture the name and title of active and deactivated Computer Linked Application Information Management System (CLAIMS3) users.

Despite the corrective actions taken, persistent data security (e.g., user access) control deficiencies put sensitive and critical DHS data at risk of unauthorized access and disclosure.[3] For example, the independent auditor's reports on DHS' financial statements and internal control over financial reporting for FYs 2016, 2017, and 2018 (Financial Statement Audit reports) identified repeated control deficiencies that put the Department's financial data at risk of unauthorized access and disclosure.[4] All three reports cited the following four deficiencies across all 3 fiscal years.

1) DHS did not adequately design, implement, and operate effective controls over initial authorization of application, database, and operating system accounts.
2) DHS did not consistently implement technical controls over logical access to key financial applications and underlying system software components.
3) DHS did not fully implement controls over the generation, review, analysis, and protection of application, database, and operating system audit logs.
4) DHS did not 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.

These conditions collectively limited DHS' ability to process, store, and report financial data in a manner that ensures accuracy, confidentiality, integrity, and availability. We also reported that DHS management did not take appropriate corrective action to address the repeated deficiencies that the independent auditor reported as a material weakness for several years.

Similarly, our annual reports on DHS' Information Security Program identified security deficiencies that continued to put DHS' sensitive data at risk of

[3] We identified 12 prior OIG reports with data security (e.g., user access) control deficiencies.
[4] *Independent Auditors' Report on DHS' FY 2016 Financial Statements and Internal Control over Financial Reporting,* OIG-17-12, November 14, 2016; *Independent Auditors' Report on DHS' FY 2017 Financial Statements and Internal Control over Financial Reporting,* OIG-18-16, November 15, 2017; and *Independent Auditors' Report on DHS' FY 2018 Financial Statements and Internal Control over Financial Reporting*, OIG-19-04, November 15, 2018.

unauthorized access and disclosure.[5] For example, a number of national security systems and unclassified systems lacked current Authority to Operate (ATO) in FYs 2016, 2017, and 2018. According to DHS and other Federal guidance, an information system must obtain an ATO before it becomes operational.[6] The ATO process provides an overarching approach for assessing the effectiveness of operational, technical, and management security controls.

We identified five additional examples where data and systems were at risk of unauthorized access and disclosure. Vulnerabilities in these areas could pose substantial threats and risks to DHS' ability to carry out its mission-critical operations. The five areas involved:

1) unmanned aircraft data in Customs and Border Protection's (CBP) Intelligence, Surveillance, and Reconnaissance Systems;[7]
2) personally identifiable data in the Office of Health Affairs' Electronic Patient Care Reporting system and BioWatch portal;[8]
3) case management and investigative data in multiple Secret Service systems;[9]
4) immigration data in USCIS' CLAIMS3;[10] and
5) cyber security data in the National Protection and Programs Directorate's unclassified and top secret Mission Operating Environment systems.[11]

Data Availability: DHS Personnel Did Not Have Essential Data Needed to Carry Out Various Mission Operations

We identified prevalent data availability issues that hindered DHS programs.[12] Most concerning, components or programs did not always capture or track data necessary for mission operations. At times, data was not readily available

[5] *Evaluation of DHS' Information Security Program for Fiscal Year 2016,* OIG-17-24, January 18 2017; *Evaluation of DHS' Information Security Program for FY 2017,* OIG-18-56, March 1, 2018; and *Evaluation of DHS' Information Security Program for Fiscal Year 2018,* OIG-19-60, September 19, 2019.
[6] *DHS Sensitive Systems Policy Directive 4300A*, July 2017; *National Institute of Standards and Technology Special Publication 800-37*, December 2018; and OMB Circular No. A-130, July 2016.
[7] *CBP Has Not Ensured Safeguards for Data Collected Using Unmanned Aircraft Systems*, OIG-18-79, September 21, 2018.
[8] *Office of Health Affairs Has Not Implemented an Effective Privacy Management Program*, OIG-18-20, November 30, 2017.
[9] *USSS Faces Challenges Protecting Sensitive Case Management Systems and Data*, OIG-17-01, October 7, 2016.
[10] *Data Quality Improvements Needed to Track Adjudicative Decisions*, OIG-19-40, May 14, 2019.
[11] *Biennial Report on DHS' Implementation of the Cybersecurity Act of 2015*, OIG-18-10, November 1, 2017.
[12] Twenty-six of 135 reports contained findings related to data availability.

on a day-to-day basis to support DHS personnel, program evaluation, or decision making. Some data was at risk of being unavailable during emergencies to support time-sensitive mission operations. Further, critical data may not have been available during service interruptions or outages to ensure continuity of operations.

To illustrate, the Department did not capture or track the information necessary for better operational decisions, program evaluation, or compliance with mandates.[13] We reported in FY 2019 that DHS faced challenges fulfilling the requirements of the *Cybersecurity Workforce Assessment Act.* Particularly, the Department's Office of the Chief Human Capital Officer faced significant challenges complying with the Act because DHS did not capture or maintain all data required to conduct workforce analysis, count and code contractor employees, or track cybersecurity training. As such, DHS was unable to assess its cybersecurity workforce or develop a workforce strategy.[14] DHS plays a critical role in protecting the Nation's cyber space, which includes its own information systems as well as those belonging to other Federal civilian agencies. Without a complete workforce assessment and strategy, DHS is not well positioned to carry out its critical cybersecurity functions in the face of ever-expanding cybersecurity threats.

Additionally, several report findings revealed instances of data not being readily available to DHS users or decision makers when needed.[15] In FY 2019, we found that the Federal Emergency Management Agency's (FEMA) information technology (IT) deficiencies hindered the ability of its workforce to effectively accomplish critical disaster response and recovery operations in the aftermath of 2017 hurricanes and wildfires.[16] Specifically, FEMA personnel faced significant challenges accessing real-time information from FEMA's data warehouse and Logistics Supply Chain Management System. The lack of real-time data slowed processing of hundreds of thousands of individual assistance applications and delivery of items such as meals and water to disaster areas.

FEMA's non-integrated systems also contributed to data availability issues by preventing efficient data tracking and exchange. For example, grants staff from a regional office had to manually review public assistance grant requests in multiple systems to verify that submitted funding requests were not duplicates. This time-consuming and manual effort resulted in grant disbursement delays of 8 months or longer. In addition, FEMA's systems did not allow for critical

[13] Twelve distinct reports disclosed that the Department did not capture or track the necessary information.

[14] *DHS Needs to Improve Cybersecurity Workforce Planning*, OIG-19-62, September 23, 2019.

[15] Eleven of the 26 reports discussed data not being readily available to DHS users or decision makers when needed.

[16] *FEMA's Longstanding IT Deficiencies Hindered 2017 Response and Recovery Operations*, OIG-19-58, August 27, 2019.

information sharing with internal and external partners, including state governments and other Federal agencies. Until FEMA upgrades its outdated and unintegrated legacy systems and inadequate equipment, its personnel will continue to struggle with manual workarounds while conducting disaster response and recovery operations.

Finally, DHS data was at risk of being unavailable during emergencies such as system outages or cybersecurity events.[17] Our annual reports on DHS' Information Security Program disclosed that the "Recover"[18] function of DHS' information security program operated below the targeted level of effectiveness during all 3 fiscal years in our review scope. Specifically, this rating was based on our assessment that DHS did not employ automated mechanisms to test system contingency plans, develop procedures for handling sensitive information, or identify alternate facilities to recover processing in the event of service disruptions. DHS components are responsible for developing and periodically testing contingency plans that outline backup and disaster recovery procedures for their respective information systems. Yet, all three OIG reports showed that DHS components had not tested contingency plans in each fiscal year for a number of systems to ensure operational restoration and recovery during an emergency. Untested contingency plans may create a false sense of security and an inability to resume operations in a timely manner.

Data Accuracy: DHS Did Not Have Optimal Data for Decision Making

Information that DHS users and other stakeholders relied upon to carry out their responsibilities was sometimes inaccurate or invalid.[19] This negatively affected many DHS mission areas, including law enforcement, border protection, immigration, financial reporting, grants management, and disaster assistance. As a result, decisions that DHS users and stakeholders made based on this information may not have been optimal for their program operations.

For example, our FY 2018 report on DHS' controls over firearms and other sensitive assets disclosed that DHS components' property records were not always accurate.[20] A physical inventory verification of 3,961 sensitive assets found that the name or physical location information for 454 assets (11 percent) did not match the information recorded in the components' inventory systems. Of the 454 assets with mismatched information, 208 were CBP

[17] Three of the 26 reports noted that DHS data was at risk of being unavailable.
[18] According to the National Institute of Standards and Technology, recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets adversely affected by cybersecurity incidents.
[19] We identified 19 reports mentioning inaccurate or invalid data.
[20] *DHS' Controls Over Firearms and Other Sensitive Assets*, OIG-18-05, October 25, 2017.

firearms that could not be physically located at a CBP regional armory. The inventory data incorrectly indicated the location of these firearms as the regional armory although they were actually located at various CBP field offices. Without accurate property records, components may be unable to provide effective oversight of their sensitive assets.

Data inaccuracies were also reported regarding DHS' financial data submitted in response to statutory requirements. One OIG report about DHS' FY 2017 conference spending[21] identified a number of data discrepancies and unsupported cost items. The *Consolidated Appropriations Act, 2017*, requires agencies to report their spending data for conferences costing more than $100,000.[22] However, the audit report indicated a total difference of $3.1 million between conference costs recorded in the Department's Conference Approval Tool and components' cost records for 85 of 86 conferences OIG sampled. Further, the Department could not substantiate acquisition and travel amounts for 39 of the 86 conferences sampled, representing a total amount of $203,660.

A second OIG report identified completeness and accuracy issues related to the Department's spending data.[23] The *Digital Accountability and Transparency Act of 2014* requires DHS to submit complete, accurate, and timely spending data to the Department of the Treasury for publication on USASpending.gov, beginning the second quarter of FY 2017. However, our sample of 385 procurement and financial assistance transaction records showed that 245 (more than 63 percent) had one or more key attributes (such as obligation amount and award date) that did not match or agree with underlying support. Despite these known completeness and accuracy issues, DHS certified its spending data in order to comply with DATA Act timeliness requirements. Without complete and accurate data, the usefulness of DHS' spending information to Congress, the public, and other stakeholders is limited.

Data Completeness and Relevance: Inadequate Data Hindered Effective Program Operations

DHS components and programs did not always have relevant or required information to ensure effective operations.[24] These data issues spanned different DHS components and mission areas including immigration, cybersecurity, financial management, and human resources management. If

[21] *Audit of Department of Homeland Security's Fiscal Year 2017 Conference Spending*, OIG-19-39, May 22, 2019.
[22] Pub. Law No. 115-31.
[23] *DHS' Implementation of the DATA Act*, OIG-18-34, December 29, 2017.
[24] Thirteen reports indicated various DHS components and programs did not have the relevant or required information needed.

not addressed, DHS users and stakeholders may not have sufficient and reliable information to provide insight into their operations or inform decision making.

For example, we reported in FY 2019 that USCIS had not implemented an effective process to track adjudicative decisions and ensure the integrity of data in CLAIMS3.[25] Specifically, the data in CLAIMS3 did not include data fields for the identity and authority of Immigration Service Officers who approved immigration benefits and did not personally record the decisions in CLAIMS3. Further, USCIS cannot link Immigration Service Officers' user identities in CLAIMS3 with serial-numbered stamps applied to enter decisions in paper files. Lacking this information, USCIS cannot compare paper and electronic records to confirm data accuracy and completeness. We also reported CLAIMS3 data did not include important data fields such as applicants' medical information that could help USCIS conduct proactive analyses to detect suspicious activities and combat fraud. These weaknesses rendered CLAIMS3 unreliable to support key immigration management activities.

In FY 2019, we also questioned the reliability of U.S. Coast Guard data concerning service members who were prohibited from carrying firearms.[26] Specifically, Coast Guard's reporting of Uniform Code of Military Justice violation and adjudication data did not capture whether the violation or outcome of a case fell under one of the prohibited categories. Coast Guard's data did not include complete information about the outcome of each case such as the verdict, sentence, or both. Additionally, Coast Guard's Uniform Code of Military Justice data did not include information about eight servicemen who had been dismissed or dishonorably discharged and were reported in the Federal Bureau of Investigations' criminal background check system. Coast Guard's incomplete data impeded its ability to readily identify service members no longer allowed to carry firearms due to prior offenses.

Data Issues Were Attributed to Various Internal Control Deficiencies

The widespread data quality issues summarized in this report can be attributed to various internal control deficiencies. Specifically, we identified 82 distinct deficiencies that hindered the confidentiality, availability, accuracy, validity, and completeness of DHS data. We grouped these 82 deficiencies into five distinct categories:

[25] *Data Quality Improvements Needed to Track Adjudicative Decisions*, OIG-19-40, May 14, 2019.

[26] *United States Coast Guard's Reporting of Uniform Code of Military Justice Violations to the Federal Bureau of Investigation*, OIG-19-22, February 21, 2019.

1) security and technical controls;
2) program and operational oversight;
3) guidelines and processes;
4) system design and functionality; and
5) training and resources.

Although the Department has implemented corrective actions to address many of the recommendations issued in our prior reports, it must also take steps to ensure the reliability, integrity, and availability of data needed to support and sustain Department operations.

Inadequate Security and Technical Controls

Security control deficiencies affected a large number of components and programs examined. According to the GAO Green Book, agency management is responsible for designing control activities over the acquisition, development, and maintenance of IT systems and using the systems development life cycle framework as a means by which to do so. However, our review identified 14 security and technical control deficiencies as causes for many of the data issues, mostly affecting data confidentiality.

Specifically, although the Department has made steady improvement in its information security program, several components continue to operate some of their national security and unclassified information systems without adequate security controls. Our annual reports on DHS' Information Security Program identified systems with unsupported operating systems, untimely security patches, or without an ATO.[27] For example, 7 National Security Systems and 24 unclassified DHS systems operated without ATO in FY 2018. In addition, 7 DHS components did not meet the required ATO target of 100 percent in FY 2018.

Additionally, the Financial Statement Audit reports for each of the fiscal years revealed that DHS did not design or implement proper controls over initial authorization of application, database, and operating system accounts.[28] The reports indicated the Department did not implement technical controls over logical access to key financial applications and underlying system software in accordance with DHS requirements. Also, the Department did not maintain appropriate segregation of duties between development and production environments. Poor access controls and inadequate segregation of duties increase the risk of current employees, separated employees, or contractors gaining unauthorized access to financial systems and data. Such access could

[27] OIG-17-24, January 18, 2017; OIG-18-56, March 1, 2018; OIG-19-60, September 19, 2019.
[28] OIG-17-12, November 14, 2016; OIG-18-16, November 15, 2017; and OIG-19-04, November 15, 2018.

lead to unauthorized activities or inappropriate disclosure of sensitive information.

The annual Financial Statement Audit reports attributed the various data deficiencies to the Department's configuration management process. Specifically, DHS did not consistently document policies and procedures for configuration management, including controls needed for system migration and upgrades. Configuration management deficiencies create vulnerabilities and increase the risk of unauthorized and undetected changes to systems, which may potentially compromise system operations and pose data reliability, validity, and completeness issues.

Inadequate Program and Operations Oversight

According to GAO's Green Book, management is responsible for assigning responsibilities, evaluating performance, and holding individuals accountable for their internal control responsibilities. Management is also responsible for using quality information to achieve the Department's objectives. We identified 19 inadequate oversight deficiencies that resulted in a number of data issues. Specifically, DHS components and headquarters did not provide effective management oversight of some programs and operations to ensure compliance with applicable guidelines and accountability for capturing and tracking complete and accurate data.

For example, in FY 2018, we reported the Immigration and Customs Enforcement (ICE) did not have adequate oversight to ensure that its main repository of known or suspected terrorist information was complete and accurate.[29] Specifically, ICE's Enforcement and Removal Operations did not clearly assign accountability for implementing the Known or Suspected Terrorist Encounter Protocol and did not perform sufficient quality control to ensure that all responsible personnel implemented it properly. As a result, data on confirmed known or suspected terrorists in Enforcement and Removal Operations' custody contained inaccurate information. Incomplete and inaccurate data on confirmed known and suspected terrorists could have a major impact on ICE's ability to protect the security of the homeland.

Inadequate Guidelines and Procedures

Management is responsible for defining responsibilities and documenting policies and procedures to ensure operational effectiveness.[30] Each component office should also document policies with the appropriate level of detail to allow

[29] *ICE Faces Challenges to Screen Aliens Who May Be Known or Suspected Terrorists*, OIG-18-36, January 5, 2018.
[30] *Standards for Internal Control in the Federal Government,* GAO-14-704G, September 2014.

management to effectively monitor the control activity. However, we identified 23 deficiencies regarding inadequate guidelines and procedures as causes for a number of data issues. Specifically, DHS management failed to develop clear program guidelines or procedures that ensured proper recording and management of essential data and verification of the accuracy and completeness of the data recorded or used. Lack of guidance and processes hindered the reliability, integrity, and availability of DHS data across different programs and components.

For example, our FY 2019 report on the Science and Technology Directorate's (S&T) Integrated Product Team process disclosed that S&T did not develop policies and procedures that included roles and responsibilities to integrate disparate research and development (R&D) data from multiple redundant tools into a single, comprehensive database.[31] As a result, S&T did not have accurate and readily available R&D data for timely reporting to the DHS Secretary and Congress. S&T missed the deadlines in 2017 and 2018 for submitting a detailed list of ongoing R&D projects to Congress as required by the *National Defense Authorization Act for FY 2017*.

System Design and Functionality Limitations

Management is responsible for designing an entity's information system to obtain and process information to meet its operational requirements and respond to objectives and risks. Prior OIG reports discussed 18 different system design or functionality limitations as causes for a number of the data issues. Specifically, several information systems were affected by design, integration, or performance issues related to capturing and sharing operational, financial, and disaster-related data. These issues hindered the reliability, integrity, and availability of DHS data across different components and missions.

For example, we disclosed in our FY 2018 report on DHS' implementation of the *Cybersecurity Act of 2015* that the system DHS used did not provide the quality, contextual data needed to effectively defend against ever-evolving cybersecurity threats.[32] Specifically, the systems supporting the Automated Indicator Sharing program that the National Protection and Programs Directorate implemented to share cyber threat indicators and defensive measures did not have the capability to provide adequate information to effectively protect Federal and private networks. This occurred because the information was produced through an automated process with pre-determined

[31] *S&T Is Not Effectively Coordinating Research and Development Efforts across DHS*, OIG-19-59, September 18, 2019.
[32] *Biennial Report on DHS' Implementation of the Cybersecurity Act of 2015*, OIG-18-10, November 1, 2017.

data fields. In addition, the National Protection and Programs Directorate's cross-domain solution for sharing unclassified and classified cyber threat indicators and defensive measures was not effective for timely sharing and analysis of cyber threat information. It also did not have automated tools for analysts to query multiple sources to enrich shared cyber threat data, resulting in potential delays in producing information for a single cyber threat indicator.

Additionally, our Financial Statement Audit reports in FYs 2017 through 2019 discussed system limitations that contributed to deficiencies in multiple DHS financial process areas.[33] Several DHS components conducted financial management with manual processes, decentralized systems, or utilities with limited automated capabilities. Consequently, these systems were not compliant with Federal financial management system requirements as defined by the *Federal Financial Management Improvement Act of 1996* and Office of Management and Budget (OMB) Circular No. A-123. These functionality limitations caused a greater risk of error and resulted in inconsistent, incomplete, or inaccurate financial controls and supporting documentation.

Inadequate Training and Resources

Management should enable employees to develop competencies appropriate for key roles, reinforce standards of conduct, and tailor training based on skill needs. However, four prior OIG reports identified instances when DHS management did not ensure key staff responsible for capturing, maintaining, and safeguarding data were properly trained to carry out their duties. Additionally, four other reports noted the Department did not have enterprise solutions in some areas and did not provide sufficient resources in other areas to ensure its components and personnel could capture and maintain the information needed for operations decisions and evaluation.

For example, our FY 2018 report on the Office of Health Affairs' (OHA) privacy safeguards indicated that OHA did not allocate adequate resources for its privacy officer to carry out required privacy management responsibilities.[34] Additionally, OHA employees and contractors were required to take annual privacy and security awareness courses and report training completion information to the DHS Privacy Office for inclusion in its quarterly reports to Congress. However, neither the OHA Privacy Office nor the Training Coordinator tracked mandatory annual privacy awareness training for all OHA

[33] OIG-17-12, November 14, 2016; OIG-18-16, November 15, 2017; and OIG-19-04, November 15, 2018.

[34] *Office of Health Affairs Has Not Implemented An Effective Privacy Management Program*, OIG-18-20, November 30, 2017.

employees. As a result, the sensitive personally identifiable information OHA collected and maintained was at risk of unauthorized access and disclosure.

Opportunities for Improvement

Even as technology rapidly advances and changes, the Department must leverage data to improve the quality of services for safeguarding the homeland. To that end, management should design information systems and controls to ensure the data recorded is accurate and valid. DHS requires the integration of quality into every phase of information management, including creation, collection, maintenance, and dissemination.

DHS' ongoing IT modernization efforts and implementation of its IT Strategic Plan and Enterprise Data Strategy offer opportunities for the Department to address the many data issues we identified in our prior reports. Implementation of the multi-year FDS and new legislative requirements also present ways for the Department to address data issues and better leverage the value of its data for mission, service, and the public good.

Information Technology Modernization

The President's Management Agenda for the 21st century identifies IT modernization as one of the key drivers of government transformation. The Agenda noted that Federal agencies can more strategically address existing needs by first determining the best prospects for modernization. The Department's *Information Technology Strategic Plan FY 2019 – 2023*, guided by the President's Management Agenda, also focuses on IT modernization.

As discussed in our FY 2019 Financial Statement Audit report, it is critical that DHS capitalize on results from prior modernization efforts, as well as corrective actions to address internal and external oversight report findings, as it moves forward with its IT modernization plans and activities. In particular, the Department should consider data issues and their causes as it moves forward to modernize its data security guidelines and network components and migrate IT applications to a cloud infrastructure.

DHS IT Strategic Plan and Enterprise Data Strategy

Also guided by the President's Management Agenda on data accountability and transparency, the Department developed its IT strategy to address both current and future technology. For example, the strategic objective to implement data protection practices to safeguard DHS systems and applications includes creating access controls and modernizing data security guidelines.

The Department's *Enterprise Data Strategy FY 2017 – 2021* also envisions driving departmental resources toward innovative data management, sharing, safeguards, and integration to fully leverage DHS' vast data assets. The five strategy goals are:

- enterprise governance;
- organization of data collection for effective mission use;
- data rules and information safeguards;
- availability and security; and
- development of a skilled data workforce to enhance longer-term mission success.

The strategy also includes guiding principles that require safeguarding data in accordance with DHS oversight requirements and relevant laws and policies. It requires DHS components use common national and international data standards for data quality, integrity, confidentiality, sharing, and availability. The Department should address access and configuration control issues as well as system design and functionality limitations as it implements the IT Strategic Plan and the Enterprise Data Strategy.

Federal Data Strategy and the Evidence Act

In FY 2019, representatives of 23 agencies across the Federal Government developed the multi-year FDS to address the President's Management Agenda priority goal of leveraging data as a strategic asset. FDS practices 11 through 14 focus on prioritizing data governance; protecting confidentiality, privacy, and data integrity; maintaining public trust; and conveying authenticity of Federal data. Additionally, one of the priority actions for 2020 was developing a data protection toolkit for maintaining confidentiality and privacy of Federal data assets. The Department should address access and configuration control issues as it implements the FDS practices and action plans.

FDS practices and action plans also include several ways to help the Department address its data quality and availability issues. For example, some FDS practices call for aligning data quality with intended use, designing data for use and re-use, maintaining data documentation, and using data to guide decision making. Other practices focus on identifying data needs to answer key agency questions, providing resources explicitly to leverage data assets, and increasing capacity for data management and analysis.

The *Evidence Act* emphasizes collaboration and coordination to advance data and evidence-building functions in the Federal Government. The *Evidence Act* statutorily mandates several actions, including ensuring open government data and protecting confidential information. The Act requires the Department to make data open by default, as well as develop a comprehensive data inventory and data catalogue. The Department will need to address the systemic control deficiencies we identified from our review as it implements the FDS and *Evidence Act* action plans in FY 2021 and beyond.

Conclusion

As the Department's *Data Quality Guide* points out, poor data quality is expensive — it costs organizations by draining money and resources as they seek to recover from errors. Improving data quality throughout its lifecycle can ensure that DHS information is well-managed and supports DHS' mission to safeguard the American people, our homeland, and our values.

DHS has made improvements to its information security program and has taken steps to improve data management over the years. The Department has developed various plans, guidance, and strategies to improve the quality and management of DHS data. It has also implemented a number of corrective actions in response to recommendations made in the prior OIG reports from FY 2017 to 2019 that we included in our review. These are good first steps, but sustained effort is needed to address the internal control issues underlying the data deficiencies we highlighted.

Management Comments and OIG Analysis

In its response to our draft report, DHS acknowledged the opportunities for continuous improvement to fully leverage its data assets, but disagreed with the report's overall conclusion. DHS also noted that we:

- did not provide specifics regarding the actions the Department has taken to address the internal control issues;
- relied upon outdated information for conclusions in the report; and
- did not mention any standards for conducting the review.

The Department also pointed out some of the progress it has made remediating issues discussed in the past OIG reports, such as completing a DHS Evidence-Based Data Strategy to improve data management and governance.

We agree that DHS has taken steps towards remediating issues we previously reported, including in our Financial Statement Audit reports. We noted in the Results of Review section, and throughout our report, that the Department has taken corrective actions to implement recommendations in our prior reports that are designed to improve financial management and information security controls. We acknowledge the Department has improved its information security program and developed various plans and strategies to improve the quality and management of its data. However, as discussed in our report, data quality issues persisted.

The Department asserts that we relied on outdated data to support conclusions in this report. The purpose of this review was to identify persistent data issues impacting DHS. As such, the focus of this review was to identify and consolidate frequently reported data issues that impacted DHS and component programs across fiscal years, regardless of recommendation statuses in past reports. For example, in our Financial Statement Audit Reports, we reported similar data issues across multiple years despite corrective actions the Department took for many of the recommendations in these reports. Specifically, the FY 2020 and FY 2021 Financial Statement Audit Reports noted the same increased risks of unauthorized access to financial systems and data due to poor access controls and inadequate segregation of duties.[35] We reported the same issues in the FY 2017 through FY 2019 reports. The risks of unauthorized and undetected changes to systems and lower assurance of data reliability were also reported as results of deficiencies in configuration management in the Financial Statement Audit Reports from FYs 2017 through 2021.

We believe this report adds value to the Department by highlighting persistent data issues and control deficiencies in spite of previously closed recommendations. The overall conclusion in this report is based on the type and frequency of the data issues we noted in our past reports during a 3-year period. We made minor edits to our overall conclusion in response to the Department's comments. We encourage the Department to consider the issues that we summarized as it develops and implements its initiatives to improve data governance and management.

The Department also asserts that this report did not mention any standards for conducting the review. We conducted this work according to the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency. We have revised Appendix A to include the

[35] *Independent Auditors' Report on DHS' FY 2019 Financial Statements and Internal Control over Financial Reporting,* OIG-20-03, November 15, 2019; and *Independent Auditors' Report on DHS' FY 2020 Financial Statements and Internal Control over Financial Reporting*, OIG-21-08, November 13, 2020.

standards we followed. We also included a copy of the Department's management comments in their entirety in Appendix B.

Appendix A
Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002*, Public Law 107−296, by amendment to the *Inspector General Act of 1978*.

We initiated this review of OIG reports issued from FY 2017 to FY 2019 to identify frequently reported findings and quantify persistent and systemic data issues that hinder DHS from carrying out its missions. To accomplish our objective, we reviewed 135 DHS OIG reports from the years in our scope to identify findings related to DHS data. We identified data issues in 48 of the 135 reports. Appendix D contains a list of the 48 reports with data issues. From the 48 reports, we identified 70 instances of data issues adversely affecting programs and components across DHS. We grouped these issues into categories based on GAO guidance on Federal information system controls and security requirements. We identified 82 different control deficiencies that hindered the confidentiality, availability, accuracy, validity, and completeness of DHS data. We grouped these control deficiencies into categories based on the commonality of the deficiencies noted.

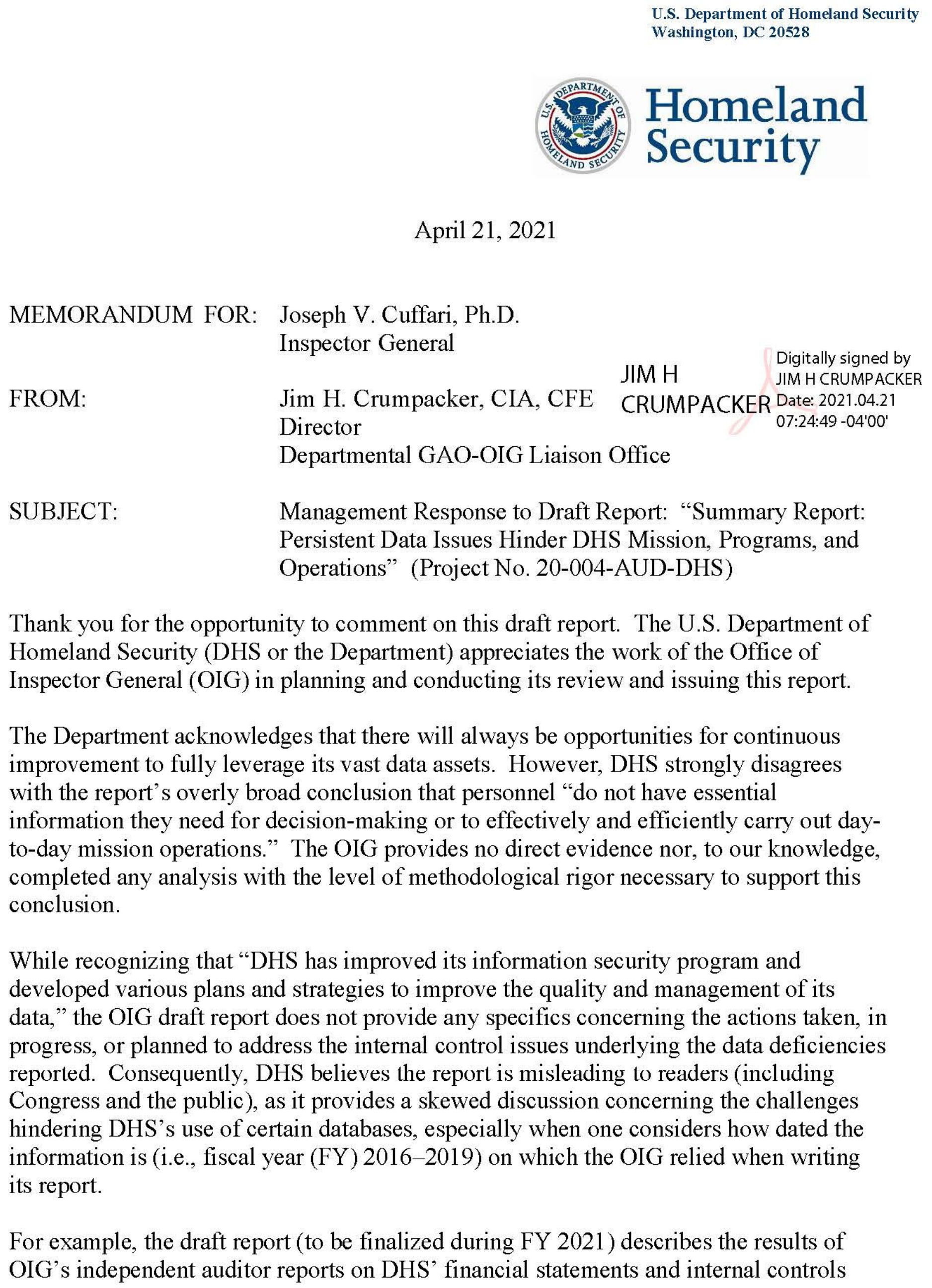
Further, we reviewed the status of recommendations made in these reports. We did not review the individual corrective actions the Department or its components implemented, or agreed to implement, in response to these recommendations.

We did not include 140 other reports issued in FYs 2017 through 2019 in our review because they either did not include fully developed findings and recommendations or were audits of FEMA's grant recipients and subrecipients. The various types of reports not included in our review were:

- Classified reports
- Summary reports
- Management alerts and letters
- Special review reports
- Verification review reports
- FEMA grant applicants' audit reports

We conducted this review between January and September 2020 pursuant to the *Inspector General Act of 1978*, as amended, and according to the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency.

Appendix B
DHS Comments to the Draft Report



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

Homeland
Security

April 21, 2021

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

FROM: Jim H. Crumpacker, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

JIM H CRUMPACKER Digitally signed by JIM H CRUMPACKER Date: 2021.04.21 07:24:49 -04'00'

SUBJECT: Management Response to Draft Report: "Summary Report: Persistent Data Issues Hinder DHS Mission, Programs, and Operations" (Project No. 20-004-AUD-DHS)

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

The Department acknowledges that there will always be opportunities for continuous improvement to fully leverage its vast data assets. However, DHS strongly disagrees with the report's overly broad conclusion that personnel "do not have essential information they need for decision-making or to effectively and efficiently carry out day-to-day mission operations." The OIG provides no direct evidence nor, to our knowledge, completed any analysis with the level of methodological rigor necessary to support this conclusion.

While recognizing that "DHS has improved its information security program and developed various plans and strategies to improve the quality and management of its data," the OIG draft report does not provide any specifics concerning the actions taken, in progress, or planned to address the internal control issues underlying the data deficiencies reported. Consequently, DHS believes the report is misleading to readers (including Congress and the public), as it provides a skewed discussion concerning the challenges hindering DHS's use of certain databases, especially when one considers how dated the information is (i.e., fiscal year (FY) 2016–2019) on which the OIG relied when writing its report.

For example, the draft report (to be finalized during FY 2021) describes the results of OIG's independent auditor reports on DHS' financial statements and internal controls over financial reporting for FYs 2016-2018, but does not include more current and readily available information. Specifically, based on the independent auditors' FY 2020 report, DHS made significant progress in remediating the conditions highlighted in the FY 2016-2018 reports, including:

- Reducing the number of findings associated with System Account Management (Authorization, Recertification, and Termination) from 42 to 26 (38 percent) since 2017, in addition to successfully removing the U.S. Customs and Border Protection (CBP) and U.S. Citizenship and Immigration Service from contributing to the Account Management condition;
- Successfully completing all CBP audit logging remediation efforts and clearing its 4 contributing findings noted in 2017; and
- Releasing detailed guidance, jointly developed by the DHS Office of the Chief Financial Officer and DHS Office of the Chief Information Security Officer, related to Account Management and Recertification as well as other areas of focus, which is supplemented by quarterly training events that include Information Technology topics offered to Component personnel across the Department.

It is also important to note that the conditions the independent auditor noted with respect to FYs 2016-2018 affected how DHS performed its mission, programs, and operations only tangentially at best. Specifically, the OIG's independent auditor has issued a clean (unmodified) audit opinion on the DHS financial statements for the past eight years. The internal control weaknesses described in the auditors' report are theoretical risks that, to-date, have not impaired decision-making or the Department's ability to effectively and efficiently carry out day-to-day activities. Nonetheless, senior DHS leadership remains committed to remediating these conditions, some of which require the implementation of new business systems and processes.

Additionally, the 45 FY 2017–2019 performance audit reports identified in Appendix D of OIG's draft report as having Data Issues (out of 132 reports reviewed[1]) lack context, thus are misleading. Specifically, 194 of 237 (82 percent) of the recommendations included in these reports were previously closed by the OIG. This clearly demonstrates the Department's commitment to continuous improvement as DHS does not close recommendations without OIG concurrence. We believe this practice provides Congress and the public added confidence that appropriate actions have been taken to implement OIG recommendations or otherwise resolve any disagreements.

[1] OIG's draft report also mentioned not including 140 other reports issued during FY 2017-2019 in its review, in part, because they "did not include fully developed findings." The Department was not sure what to make of this statement.

In September 2020, DHS also established the standalone Chief Data Officer (CDO) Directorate (previously part of the Chief Technology Officer Directorate), pursuant to the "Foundations for Evidence-Based Policymaking Act of 2018" (Evidence Act). The CDO focuses squarely on: (1) life cycle data management; (2) data access; (3) data security; (4) data governance; and (5) data usage. Further, there are a number of activities in progress, including:

- Completing a DHS Evidence-Based Data Strategy to align with the Evidence Act;
- Establishing a DHS Data Governance Council Charter to implement standardization and align with National Information Exchange Model Standards;
- Finalizing a DHS Maturity Model to assess the maturity of the DHS Data Domains;
- Finalizing a DHS Data Domain Structure to support a robust data governance model;
- Developing a DHS Open Data Plan ensuring open government data and protecting confidential information; and
- Completing the DHS data inventory and finalizing Data Sharing Agreements.

DHS remains committed to maturing Enterprise Data Management across the Department. This includes: (1) supporting Components' effective and efficient mission delivery; (2) advancing integrated analytic capabilities; (3) reducing duplicated data; and (4) facilitating data-informed decision making.

The OIG chose not to include any recommendations in this report, although stated "… follow-through and continued improvement will be essential to address the internal control issues underlying the data deficiencies we highlighted." DHS welcomes OIG's specific actionable recommendations.

The Department also noted the OIG's statement "We did not comply with generally accepted government auditing standards [GAGAS] in conducting our review." It appears that OIG's work also did not comply with Council of the Inspectors General on Integrity and Efficiency (CIGIE) Inspection and Evaluation Standards, as these were not mentioned in the draft report. DHS generally has a higher level of confidence in OIG work that adheres to GAGAS or CIGIE inspection and evaluation standards.

Again, thank you for the opportunity to review and comment on this draft report. DHS previously submitted technical comments under a separate cover for OIG's consideration. Please feel free to contact me if you have any questions.

Appendix C
Summary of Data Issues and Causes

Table 1. Summary of Data Issues Identified

FY	Access Issues	Availability Issues	Accuracy & Validity Issues	Completeness Issues
2017	3	8	7	1
2018	5	10	6	7
2019	4	8	6	5
Total	12	26	19	13

Source: Review of FY 2017 through FY 2019 DHS OIG reports

Table 2. Summary of Causes Identified

FY	IT Control Deficiencies	Inadequate Oversight	Systems Limitations	Inadequate Guidance & Procedures	Inadequate Training & Resources
2017	6	4	6	3	2
2018	5	12	7	6	2
2019	3	3	5	14	4
Total	14	19	18	23	8

Source: Review of FY 2017 through FY 2019 DHS OIG reports

Appendix D
FYs 2017–2019 DHS OIG Reports with Data Issues

DHS OIG Reports	Access	Availability	Completeness	Accuracy	Validity
OIG-17-01 *USSS Faces Challenges Protecting Sensitive Case Management Systems and Data*	1				
OIG-17-05 *DHS Is Slow to Hire Law Enforcement Personnel*		1		1	
OIG-17-11 *Better Safeguards Are Needed in USCIS Green Card Issuance*				1	
OIG-17-114 *CBP's IT Systems and Infrastructure Did Not Fully Support Border Security Operations*		1		1	
OIG-17-119 *ICE Field Offices Need to Improve Compliance with Oversight Requirements for Segregation of Detainees with Mental Health Conditions*		1		1	
OIG-17-12 *Independent Auditors' Report on DHS' FY 2016 Financial Statements and Internal Control over Financial Reporting*	1				
OIG-17-22 *DHS Lacks Oversight of Component Use of Force* (Redacted)		1	1	1	
OIG-17-24 *Evaluation of DHS' Information Security Program for Fiscal Year 2016*	1	1			
OIG-17-42 *H-2 Petition Fee Structure is Inequitable and Contributes to Processing Errors*		1			

OIG-17-51 *ICE Deportation Operations*		1			
OIG-17-56 *DHS Tracking of Visa Overstays Is Hindered by Insufficient Technology*		1		1	
OIG-17-60 *CBP Continues to Improve Its Ethics and Integrity Training, but Further Improvements are Needed*				1	
OIG-18-03 *USCIS Needs a Better Approach to Verify H-1B Visa Participants*			1		
OIG-18-05 *DHS' Controls over Firearms and Other Sensitive Assets*		1	1	1	
OIG-18-07 *DHS Needs a More Unified Approach to Immigration Enforcement and Administration*		1			
OIG-18-10 *Biennial Report on DHS' Implementation of the Cybersecurity Act of 2015*	1	1	1		
OIG-18-13 *FEMA and CBP Oversight of Operation Stonegarden Program Needs Improvement*		1		1	
OIG-18-15 *Coast Guard IT Investments Risk Failure without Required Oversight*			1		
OIG-18-16 *Independent Auditors' Report on DHS' FY 2017 Financial Statements and Internal Control over Financial Reporting*	1				
OIG-18-19 *Review of CBP Information Technology System Outage of January 2, 2017* (Redacted)		1			

OIG-18-20	1				
Office of Health Affairs Has Not Implemented an Effective Privacy Management Program					
OIG-18-23				1	
USCIS Has Been Unsuccessful in Automating Naturalization Benefits Delivery					
OIG-18-34			1	1	
DHS' Implementation of the DATA Act					
OIG-18-36			1	1	
ICE Faces Challenges to Screen Aliens Who May Be Known or Suspected Terrorists (Redacted)					
OIG-18-41		1			
DHS Needs to Strengthen Its Suspension and Debarment Program					
OIG-18-56	1	1			
Evaluation of DHS' Information Security Program for FY 2017					
OIG-18-58					1
USCIS Has Unclear Website Information and Unrealistic Time Goals for Adjudicating Green Card Applications					
OIG-18-73		1			
DHS Non-disclosure Forms and Settlement Agreements Do Not Always Include the Required Statement from the Whistleblower Protection Enhancement Act of 2012					
OIG-18-76			1		
Assaults on CBP and ICE Law Enforcement Officers					
OIG-18-79	1				
CBP Has Not Ensured Safeguards for Data Collected Using Unmanned Aircraft Systems					

OIG-18-80 *Progress Made, but CBP Faces Challenges Implementing a Biometric Capability to Track Air Passenger Departures Nationwide*		1			
OIG-18-81 *DHS Support Components Do Not Have Sufficient Processes and Procedures to Address Misconduct*		1			
OIG-19-04 *Independent Auditors' Report on DHS' FY 2018 Financial Statements and Internal Control over Financial Reporting*	1				
OIG-19-10 *CBP's Searches of Electronic Devices at Ports of Entry* (Redacted)	1				
OIG-19-14 *Oversight Review of the Department of Homeland Security Immigration and Customs Enforcement, Office of Professional Responsibility, Investigations Division*				1	
OIG-19-18 *ICE Does Not Fully Use Contracting Tools to Hold Detention Facility Contractors Accountable for Failing to Meet Performance Standards*		1			
OIG-19-22 *United States Coast Guard's Reporting of Uniform Code of Military Justice Violations to the Federal Bureau of Investigation*			1		
OIG-19-23 *Border Patrol Needs a Staffing Model to Better Plan for Hiring More Agents*				1	
OIG-19-28 *ICE Faces Barriers in Timely Repatriation of Detained Aliens*		1	1		

OIG-19-39			1	1	
Audit of Department of Homeland Security's Fiscal Year 2017 Conference Spending					
OIG-19-40	1		1	1	
Data Quality Improvements Needed to Track Adjudicative Decisions					
OIG-19-48		1	1		
DHS Needs to Improve Its Oversight of Misconduct and Discipline					
OIG-19-56				1	
TSA's Data and Methods for Classifying Its Criminal Investigators as Law Enforcement Officers Need Improvement					
OIG-19-58		1		1	
FEMA's Longstanding IT Deficiencies Hindered 2017 Response and Recovery Operations					
OIG-19-59		1			
S&T Is Not Effectively Coordinating Research and Development Efforts across DHS					
OIG-19-60	1	1			
Evaluation of DHS' Information Security Program for Fiscal Year 2018					
OIG-19-62		1			
DHS Needs to Improve Cybersecurity Workforce Planning					
OIG-19-66		1			
FEMA Did Not Sufficiently Safeguard Use of Transportation Assistance Funds					
Grand Total	**12**	**26**	**13**	**18**	**1**

Appendix E
Office of Audits Major Contributors to This Report

Tuyet-Quan Thai, Director
Johnson Joseph, Manager
Scott Schwemin, Program Analyst
Heather Newton, Program Analyst
Thomas Hamlin, Communications Analyst
Melissa Brown, Independent Reference Reviewer

Appendix F
Report Distribution

Department of Homeland Security

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