Office of the Inspector General:

Review of Seven Offices

Compiled and Edited by

Michael Erbschloe

Connect with Michael on LinkedIn

Table of Contents

About the Editor

Michael Erbschloe has worked for over 30 years performing analysis of the economics of information technology, public policy relating to technology, and utilizing technology in reengineering organization processes. He has authored several books on social and management issues of information technology that were published by McGraw Hill and other major publishers. He has also taught at several universities and developed technology-related curriculum. His career has focused on several interrelated areas:

- Technology strategy, analysis, and forecasting
- Teaching and curriculum development
- Writing books and articles
- Publishing and editing
- Public policy analysis and program evaluation

Books by Michael Erbschloe

Extremist Propaganda in Social Media: A Threat to Homeland Security (CRC Press)
Threat Level Red: Cybersecurity Research Programs of the U.S. Government (Auerbach Publications)
Social Media Warfare: Equal Weapons for All (Auerbach Publications)
Walling Out the Insiders: Controlling Access to Improve Organizational Security (Auerbach Publications)
Physical Security for IT (Elsevier Science)
Trojans, Worms, and Spyware (Butterworth-Heinemann)
Implementing Homeland Security in Enterprise IT (Digital Press)
Guide to Disaster Recovery (Course Technology)
Socially Responsible IT Management (Digital Press)
Information Warfare: How to Survive Cyber Attacks (McGraw Hill)
The Executive's Guide to Privacy Management (McGraw Hill)
Net Privacy: A Guide to Developing & Implementing an e-business Privacy Plan (McGraw Hill)

Introduction

The CIGIE is comprised of all Inspectors General whose offices are established under section 2 or section 8G of the Inspector General Act of 1978 (5 U.S.C. App.), those that are Presidentially-appointed/Senate Confirmed and those that are appointed by agency heads (designated federal entities). The Deputy Director for Management of the Office of Management and Budget is the Executive Chair of the Council. The Chair of the Council is elected by the Council members to serve a 2 year term. The Chair appoints a Vice Chair from other than the category from which the Chair was elected. Other statutory members of the CIGIE include: the Inspectors General of the Office of the Director of National Intelligence and the Central Intelligence Agency, the Controller of the Office of Federal Financial Management, a senior level official of the Federal Bureau of Investigation designated by the Director of the Federal Bureau of Investigation, Director of the Office of Government Ethics, Special Counsel of the Office of Special Counsel, the Deputy Director of the Office of Personnel Management, the Inspectors General of the Library of Congress, Capitol Police, Government Publishing Office, Government Accountability Office, and the Architect of the Capitol.

Prior to the establishment of the CIGIE, the Federal Inspectors General operated under the auspices of two councils, The President's Council on the Integrity and Efficiency (PCIE) and the Executive Council on the Integrity and Efficiency (ECIE) from the time they were established by Executive Order 12805, May 11, 1992 until the signing of P.L. 110-409.

The Council of the Inspectors General on Integrity and Efficiency (CIGIE) was statutorily established as an independent entity within the executive branch by the "The Inspector General Reform Act of 2008," P.L. 110-409 to:

- Address integrity, economy, and effectiveness issues that transcend individual Government agencies; and
- Increase the professionalism and effectiveness of personnel by developing policies, standards, and approaches to aid in the establishment of a well-trained and highly skilled workforce in the offices of the Inspectors General.

To accomplish its mission, the CIGIE:

- Continually identify, review, and discuss areas of weakness and vulnerability in Federal programs and operations with respect to fraud, waste, and abuse;
- Develop plans for coordinated, Government wide activities that address these problems and promote economy and efficiency in Federal programs and operations, including interagency and inter-entity audit, investigation, inspection, and evaluation programs and projects to deal efficiently and effectively with those problems concerning fraud and waste that exceed the capability or jurisdiction of an individual agency or entity;
- Develop policies that will aid in the maintenance of a corps of well-trained and highly skilled Office of Inspector General personnel;
- Maintain an Internet website and other electronic systems for the benefit of all Inspectors General;
- Maintain 1 or more academies as the Council considers desirable for the professional training of auditors, investigators, inspectors, evaluators, and other personnel of the various offices of Inspector General;

- Submit recommendations of individuals to the appropriate appointing authority for any appointment to an office of Inspector General described under subsection (b)(1)(A) or (B);
- Make such reports to Congress as the Chairperson determines are necessary or appropriate; and
- Perform other duties within the authority and jurisdiction of the Council, as appropriate.

Annual Reports on the Top Management and Performance Challenges

Each year, federal Inspectors General (IGs) identify and report on the top management and performance challenges (TMPC) facing their individual agencies pursuant to the Reports Consolidation Act of 2000.1 In addition, the Council of the Inspectors General on Integrity and Efficiency (CIGIE) issues an Annual Report to the President and Congress that includes a list of the top management and performance challenges shared by many federal agencies. Many of the identified challenges remain the same each year and can be found in agencies throughout the federal government, despite vast differences in size and mission.

The objective of this report is to consolidate and provide insight into the most frequently reported challenges identified by federal, statutory Offices of Inspector General (OIGs) based on work conducted in the previous fiscal year (FY). The report also may serve to assist policymakers in determining how best to address these challenges in the future. Even though the broad categories of challenges may remain the same over time, the specific areas of concern may change from year to year, based on the federal government's progress in addressing certain aspects of the challenges, changing priorities, and emerging risks.

To accomplish this objective, OIG reviewed TMPC reports that were issued by federal, statutory OIGs in the previous FY. Specifically, reviewing every challenge reported in each TMPC report to ascertain whether it fell within one of the broad categories identified in the CIGIE Annual Report to the President and Congress or fell into another broad category. Through this process, the most frequently reported challenges by category are identified. Note that this methodology resulted in a number of extremely important challenges that were cited by several OIGs, such as those related to national security, public safety, and public health, not being included in this report because they did not rank among the challenges most frequently reported by the 61 OIGs, primarily because only a limited number of those OIGs have oversight responsibilities in these areas. Their absence in this report does not reflect a qualitative judgment about the impact or importance of these challenges. OIG top management and performance challenges reports reviewed were:

Amtrak
Appalachian Regional Commission
Architect of the Capitol
Board of Governors of the Federal Reserve System
Broadcasting Board of Governors
Chemical Safety and Hazard Investigation Board

Committee for Purchase From People Who Are Blind or Severely Disabled (AbilityOne Program)
Consumer Financial Protection Bureau
Consumer Product Safety Commission
Corporation for National and Community Service
Defense Nuclear Facilities Safety Board
Denali Commission
Department of Agriculture
Department of Commerce
Department of Defense
Department of Education
Department of Energy
Department of Health and Human Services
Department of Homeland Security
Department of Housing and Urban Development
Department of Justice
Department of Labor
Department of State
Department of the Interior
Department of the Treasury
Department of Transportation
Department of Veterans Affairs
Election Assistance Commission
Environmental Protection Agency
Equal Employment Opportunity Commission
Export-Import Bank of the United States
Farm Credit Administration
Federal Election Commission
Federal Housing Finance Agency
Federal Labor Relations Authority
Federal Maritime Commission
Federal Trade Commission
General Services Administration
Government Publishing Office
Gulf Coast Ecosystem Restoration Council
Internal Revenue Service (Treasury Inspector General for Tax Administration)
Library of Congress
National Aeronautics and Space Administration
National Archives and Records Administration
National Endowment for the Arts
National Endowment for the Humanities
National Labor Relations Board
National Science Foundation
Nuclear Regulatory Commission
Office of Personnel Management
Peace Corps

Pension Benefit Guaranty Corporation
Railroad Retirement Board
Securities and Exchange Commission
Small Business Administration
Social Security Administration
Special Inspector General for Troubled Asset Relief Program
U.S. Agency for International Development
U.S. Commodity Futures Trading Commission
U.S. International Trade Commission
U.S. Postal Service

Many IGs reported that their agencies' challenges were impacted by resource issues, both human and budgetary. For example, the inadequate allocation of funding directly impacted the challenges related to Information Technology Security and Management, Human Capital Management, and Facilities Maintenance. Similarly, the inability to hire, recruit, train, and/or retain personnel who have the skills needed to efficiently and effectively execute federal agencies' missions directly impacts the Information Technology Security and Management, Human Capital Management, and Procurement Management challenges. In addition, OIGs reported that federal agencies' failure to use performance-based metrics to assess the success of their programs and operations negatively impacted the Performance Management and Accountability, Procurement Management, and Grant Management challenges.

The **information technology (IT) security and management challenge** includes TMPC challenges related to (1) the protection of federal IT systems from intrusion or compromise by external or internal entities and (2) the planning and acquisition for replacing or upgrading IT infrastructure. This is a long-standing, serious, and ubiquitous challenge for federal agencies across the government, because agencies depend on reliable and secure IT systems to perform their mission-critical functions. The security and management of government IT systems remain challenges due to significant impediments faced by federal agencies, including resource constraints and a shortage of cybersecurity professionals.

Key areas of concern are safeguarding sensitive data and information systems, networks, and assets against cyber-attacks and insider threats; modernizing and managing federal IT systems; ensuring continuity of operations; and recruiting and retaining a highly skilled cybersecurity workforce.

Federal information systems continue to be targets of cyber-attacks and vulnerable to insider threats. In the face of this ever-present and ever-escalating threat, federal agencies across the government face challenges in ensuring information systems are secure and sensitive data is protected. Given the immense responsibilities with which federal agencies are charged, failure to meet this challenge can have significant consequences in any number of ways, including by exposing individuals' personal information and compromising national security. For instance, in 2015, data breaches at the Office of Personnel Management exposed the personal information of over 20 million people.

The Social Security Administration (SSA) OIG reported deficiencies in the agency's ability to protect the confidentiality, integrity, and availability of the SSA's information systems and data. The SSA OIG recommended that the SSA should make protecting its network and information system a top priority and dedicate the resources needed to ensure the appropriate design and operating effectiveness of information security controls and prevent unauthorized access to sensitive information. Compounding this challenge, some agencies, including the Department of Commerce (DOC) and Department of Justice (DOJ), have encountered difficulty sharing information regarding cybersecurity threats with internal and external stakeholders because the information is often either classified or extremely sensitive.

Some OIGs expressed a concern with agencies' efforts to detect and mitigate the impact of insider threats. The Department of Defense (DOD) OIG noted that despite the DOD's efforts to limit insider risks, two contractors working for the National Security Agency removed classified information in 2017, and, in at least one instance, disclosed classified information. Across the government, progress in addressing the challenge of safeguarding data and information systems can be impeded by limited resources. The Export-Import Bank of the United States (EXIM) OIG stated that limited budgetary resources have posed a challenge for EXIM in developing, implementing, and maintaining a mature information security program.

Outdated or obsolete IT systems can potentially reduce system reliability and affect an agency's ability to fulfill its mission. Many OIGs found that their respective agencies were using legacy IT systems to perform core functions and responsibilities. For instance, the Treasury Inspector General for Tax Administration (TIGTA) stated that the Internal Revenue Service (IRS) has a large and increasing amount of aged hardware, some of which is three to four times older than industry standards. In its FY 2016 President's Budget, the IRS noted that its information technology infrastructure poses significant risk of failures due to its reliance on legacy systems and use of outdated programming languages. However, it is unknown when these failures will occur, how severe they will be, or whether they will have material impacts on tax administration during a filing season.

Outdated IT systems can also impact the security of the agency. The DOJ OIG reported that the DOJ's Justice Security Operations Center, which provides 24/7 monitoring of the DOJ's internet gateways and incident response management, is hampered by its aging infrastructure, some of which is past its end of useful life and is no longer supported.

The cost of maintaining legacy IT systems has also inhibited efforts to develop and implement updated IT systems, as agencies are forced to grapple with limited budgets and competing priorities. In particular, the SSA OIG stated that the SSA spent $1.8 billion on IT in fiscal year 2017. However, according to the SSA, budget constraints have forced SSA to use much of its IT funding to operate and maintain existing systems.

In addition, the failure to improve and modernize IT systems can threaten national security. The Department of Homeland Security (DHS) OIG found that the slow performance of a critical pre-screening system greatly reduced U.S. Customs and Border Protection (CBP) officers' ability to identify passengers who may be of concern, and frequent network outages hindered air and marine surveillance operations.

Some OIGs have noted deficiencies with agency IT contingency planning. The Department of the Interior (DOI) OIG, for example, has highlighted agency data backup issues, which could potentially leave DOI without access to important data should a computer fail or system be compromised. Similarly, the Department of State (State) OIG found that IT contingency plans for some overseas posts failed to meet departmental guidelines, which could negatively affect a post's ability to recover from an IT incident.

Compounding these issues, many federal agencies face challenges in attracting and retaining a highly skilled cybersecurity workforce to help mitigate attacks and protect federal agencies from cyber intrusions. A significant impediment for agencies in expanding the federal cybersecurity workforce is a shortage of available cybersecurity professionals. For example, the Department of Transportation (DOT) OIG stated that federal and private sector demand for cybersecurity professionals is outpacing supply by approximately 40,000 jobs in the United States.

The **performance management and accountability challenge** includes challenges related to managing agency programs and operations efficiently and effectively to accomplish mission-related goals. Although federal agencies vary greatly in size and mission, they face some common challenges in improving performance in agency programs and operations. Key areas of concern include collecting and using performance-based metrics; overseeing private-sector corporations' impact on human health, safety, and the economy; and aligning agency component operations to agency-wide goals.

Agencies also face challenges related to their responsibilities for conducting oversight of private-sector products or services that could have impacts on human health, safety, and economic viability. Effective oversight not only improves the operations of the agency in question; it also directly affects the experience of citizens, businesses, and organizations that depend on these products and services. For example, the DOT OIG reported that DOT continues to face new and longstanding oversight challenges to ensure safety efforts keep pace with the rapidly evolving airline industry. Among them is DOT's effort to oversee the manufacture and repair of aircraft parts according to federal standards. Similarly, the Department of Health and Human Services (HHS) OIG noted HHS's challenge in overseeing the safety of drugs and medical devices. Specifically, HHS OIG stated that the intricate global supply chains for drugs and medical devices present HHS with many challenges, and the products are at risk of diversion, theft, counterfeiting, and adulteration. The Department of Labor (DOL) OIG reported on DOL's challenge in enforcing laws to protect workers from death, injury, and illness in high-risk industries such as construction, forestry, fishing, agriculture, and mining. The Securities and Exchange Commission (SEC) OIG reported an immediate and pressing need for ensuring sufficient examination coverage of registered investment advisors. The Board of Governors of the Federal Reserve System (FRB) continues to take measures to enhance its oversight framework for banking organizations and will have to be sufficiently nimble to respond to changes that could influence the strategic direction of its supervisory efforts.

The **human capital management challenge** includes TMPC challenges related to recruiting, managing, developing, and optimizing agency human resources. Human capital management is a significant challenge that impacts the ability of federal agencies to meet their performance goals

and to execute their missions efficiently. Consistent with the findings of the IG community, GAO has identified strategic human capital management within the federal government as a high-risk area since 2001. Key areas of concern include inadequate funding and staffing; recruiting, training, and retaining qualified staff; agency cultures that negatively impact the agency's mission; and the impact of the lack of succession planning and high employee turnover.

The lack of adequate, predictable funding and staffing can negatively affect an agency's ability to meet its mission. Further, the necessity of operating under Continuing Resolutions and complying with hiring freezes result in budget uncertainties, delayed hiring actions, and overworked agency staffs. The National Labor Relations Board (NLRB) OIG reported that reduced or flat appropriations and the loss of key personnel through retirements directly affect the NLRB's ability to maintain a stable and productive workforce. Similarly, the U.S. AbilityOne Commission (AbilityOne) OIG reported that AbilityOne does not have adequate staffing and resources to effectively execute its responsibilities and sustain its mission. AbilityOne OIG further reported that its agency faces challenges as it operates with a staff of less than 31 people responsible for administering a $3 billion program with locations in all 50 states, Puerto Rico, and Guam.

The **financial management challenge** includes challenges related to a broad range of functions, from program planning, budgeting, and execution to accounting, audit, and evaluation. Weaknesses in any of these functional areas limit an agency's ability to ensure that taxpayer funds are being used efficiently and effectively and constitute a significant risk to federal programs and operations. Key areas of concern include both the need for agencies to improve their financial reporting and systems, and the significant amount of dollars federal agencies lose through improper payments.

As government programs and operations continue to grow in complexity, stringent reporting requirements become increasingly necessary to ensure program integrity, efficiency, and transparency. However, agencies' ability to track and report financial data has not kept pace with agency needs. In particular, outdated financial management systems may not have the configurations necessary to track and report financial data reliably as agency needs evolve, making effective financial management difficult. For example, some OIGs reported on agencies' challenges complying with regulatory changes and modernization requirements, such as the Digital Accountability and Transparency Act of 2014 (Public Law No. 113-01) that established new financial reporting requirements for all federal agencies. Multiple OIGs also reported deficiencies in the internal controls over their agencies' financial management reporting and systems, such that the agencies' ability to report reliable financial information was impacted. In some instances, OIGs found that these deficiencies rose to the level of material weaknesses in internal controls over financial reporting, meaning that there was a reasonable possibility that a material misstatement of an agency's financial statement would not be prevented or detected on a timely basis.

The **procurement management challenge** encompasses the entire procurement process, including pre-award planning, contract award, and post-award contract administration. Given that the federal government awarded over $500 billion in contracts in FY 2017, the fact that many federal agencies face challenges in Procurement Management indicates that billions of

taxpayer dollars may be at increased risk for fraud, waste, abuse and mismanagement. Further, many federal agencies rely heavily on contractors to perform their missions and, as a result, the failure of a federal agency to efficiently and effectively manage its procurement function could also impede the agency's ability to execute its mission. Key areas of concern for this challenge include weaknesses with procurement planning, managing and overseeing contractor performance, and the training of personnel involved in the procurement function.

Federal **agencies face challenges ensuring that their facilities stay in proper condition** and remain capable of fulfilling the government's needs. Throughout the federal government, OIGs have identified insufficient funding as the primary reason why agencies fail to maintain and improve their equipment and infrastructure. Without additional funding for required maintenance and modernization, it is unclear how agencies will manage the challenges of equipment and infrastructure that are simultaneously becoming more costly and less effective. Key areas of concern related to facilities maintenance are the increased likelihood of mission failure and the higher overall cost of deferred maintenance.

Promptly addressing maintenance needs reduces the chance of structural failures that may impact whether an agency can accomplish its mission. In some cases, agencies are dealing with deteriorating infrastructure that may cause substandard working conditions for staff, create inconveniences in using equipment, fail to incorporate newer technologies and standards, or cause other issues. In other, more significant cases, agencies may be hampered in performing their missions effectively because of breakdowns in essential equipment or hazards posed by unmaintained infrastructure. For example, the DOE OIG noted its Department had reported that only 50 percent of its structures and facilities were considered functionally adequate to meet the mission. Additionally, a DOD report stated that in order to remain safe, secure, and effective, the U.S. nuclear stockpile must be supported by a modern physical infrastructure, but the DOE OIG noted that the average age of its Department's facilities, which support the nuclear stockpile, is 36 years.

The **grant management challenge** includes challenges related to the process used by federal agencies to award, monitor, and assess the success of grants. Deficiencies in any of these areas can lead to misspent funds and ineffective programs. As proposed in the President's budget for FY 2018, federal agencies will spend more than $700 billion through grants to state and local governments, non-profits, and community organizations to accomplish mission-related goals. However, the increasing number and size of grants has created complexity for grantees and made it difficult for federal agencies to assess program performance and conduct oversight. Even though the key areas of concern relating to the grant management challenge overlap with issues discussed in other challenges, such as the Performance Management and Accountability and the Financial Management sections, OIGs reported grant management as a TMPC with sufficient frequency that it ranked as a separate, freestanding challenge. Key areas of concern are ensuring grant investments achieve intended results, overseeing the use of grant funds, and obtaining timely and accurate financial and performance information from grantees.

U.S. Department of Health and Human Services OIG

The Department of Health and Human Services (HHS) Office of the Inspector General (OIG) is the largest inspector general's office in the Federal Government, with approximately 1,600 dedicated to combating fraud, waste and abuse and to improving the efficiency of HHS programs. A majority of OIG's resources goes toward the government oversight of Medicare and Medicaid—programs that represent a significant part of the Federal budget and that affect this country's most vulnerable citizens. OIG's oversight extends to programs under other HHS institutions, including the Centers for Disease Control and Prevention, National Institutes of Health, and the Food and Drug Administration.

OIG provides independent and objective oversight of more than 300 HHS programs, which represent 24 cents of every Federal dollar spent. For more than 30 years, OIG has consistently achieved commendable results and significant returns on investment. In FY 2012 alone, OIG's efforts resulted in estimated savings and expected recoveries of misspent funds totaling approximately $15.4 billion. The Health Care Fraud and Abuse Control program, of which OIG is a key partner, returned more than $7 for every $1 invested. Such results are increasingly important as the Federal Government works to improve the effectiveness and efficiency of its operations and to provide services of the highest quality. This Strategic Plan will guide OIG efforts over the coming years.

Mission. OIG's mission is to protect the integrity of HHS programs and the health and welfare of the people they serve. As established by the Inspector General Act of 1978, OIG is an independent and objective organization that fights fraud, waste, and abuse and promotes efficiency, economy, and effectiveness in HHS programs and operations and works to ensure that Federal dollars are used appropriately and that HHS programs well serve the people who use them.

Vision. The vision is to drive positive change in HHS programs and in the lives of the people served by these programs. OIG pursues this vision through independent oversight of HHS programs and operations and by providing HHS and Congress with objective and reliable information for use in policymaking. They assess the Department's performance, administrative operations, and financial stewardship. They evaluate risks to HHS programs and the people they serve, and recommend improvements. The law enforcement component of OIG investigates fraud and abuse against HHS programs and holds wrongdoers accountable for their actions.

Values. OIG strives to be relevant, impactful, customer-focused, and innovative and applies these values to our work in order to persuade others to take action by changing rules, policies, and behaviors to improve HHS programs and operations. OIG strives to serve as a model for good government. Of key importance is engagement with our stakeholders—Congress, HHS, health and human services professionals, and consumers—to understand their needs, challenges, and interests in order to develop and identify areas for closer scrutiny and offer recommendations for improvement. OIG does this throughout the year, but most visibly through the development of the annual *Work Plan* and HHS's *Top Management and Performance Challenges*. The goals, priorities, and strategies in these documents reflect the ongoing stakeholder engagement and the assessment of the input received.

HHS OIG's goals and priorities reflect the positive changes toward which they strive:

Goal One: Fight Fraud, Waste, and Abuse

- Identify, investigate, and take action when needed
- Hold wrongdoers accountable and maximize recovery of public funds
- Prevent and deter fraud, waste, and abuse

Goal Two: Promote Quality, Safety, and Value

- Foster high quality of care
- Promote public safety
- Maximize value by improving efficiency and effectiveness

Goal Three: Secure the Future

- Foster sound financial stewardship and reduction of improper payments
- Support a high-performing health care system
- Promote the secure and effective use of data and technology

Goal Four: Advance Excellence and Innovation

- Recruit, retain, and empower a diverse workforce
- Leverage leading-edge tools and technology
- Promote leadership, vision, and expertise

Top 12 Management and Performance Challenges Facing HHS

1. Preventing and Treating Opioid Misuse
2. Ensuring Program Integrity in Medicare Fee-for-Service and Effective Administration of Medicare
3. Ensuring Program Integrity and Effective Administration of Medicaid
4. Ensuring Value and Integrity in Managed Care and Other Innovative Healthcare Payment and Service Delivery Models
5. Protecting the Health and Safety of Vulnerable Populations
6. Improving Financial and Administrative Management and Reducing Improper Payments
7. Protecting the Integrity of HHS Grants
8. Ensuring the Safety of Food, Drugs, and Medical Devices
9. Ensuring Quality and Integrity in Programs Serving American Indian/Alaska Native Populations
10. Protecting HHS Data, Systems, and Beneficiaries from Cybersecurity Threats
11. Ensuring that HHS Prescription Drug Programs Work as Intended
12. Ensuring Effective Preparation and Response to Public Health Emergencies

The OIG Work Plan sets forth various projects including OIG audits and evaluations that are underway or planned to be addressed during the fiscal year and beyond by OIG's Office of Audit Services and Office of Evaluation and Inspections. Projects listed in the Work Plan span the Department and include the Centers for Medicare & Medicaid Services (CMS), public health agencies such as the Centers for Disease Control and Prevention (CDC) and National Institutes of Health (NIH), and human resources agencies such as Administration for Children and Families (ACF) and the Administration on Community Living (ACL). OIG also plans work related to issues that cut across departmental programs, including State and local governments' use of Federal funds, as well as the functional areas of the Office of the Secretary of Health & Human Services (HHS). Some Work Plan items reflect work that is statutorily required.

OIG operates by providing independent and objective oversight that promotes economy, efficiency, and effectiveness in the programs and operations of HHS. OIG's program integrity and oversight activities adhere to professional standards established by the Government Accountability Office (GAO), Department of Justice (DOJ), and the Inspector General community. OIG carries out its mission to protect the integrity of HHS programs and the health and welfare of the people served by those programs through a nationwide network of audits, investigations, and evaluations, as well as outreach, compliance, and educational activities.
How We Plan Our Work

OIG assess relative risks in HHS programs and operations to identify those areas most in need of attention and, accordingly, to set priorities for the sequence and proportion of resources to be allocated. Audits and evaluations may be cancelled based on OIG staff availability, changes in the environment, legislation that substantially affects the issue or similar recent studies that provided definitive results. Reports are cancelled only after senior staff have reviewed and approved the cancellation. In evaluating potential projects to undertake, OIG considers a number of factors, including:

- mandatory requirements for OIG reviews, as set forth in laws, regulations, or other directives;
- requests made or concerns raised by Congress, HHS management, or the Office of Management and Budget;
- top management and performance challenges facing HHS;
- work performed by other oversight organizations (e.g., GAO);
- management's actions to implement OIG recommendations from previous reviews; and
- potential for positive impact.

The report entitled “The Food and Drug Administration's Policies and Procedures Should Better Address Post market Cybersecurity Risk to Medical Devices” 10-29-2018 | Audit (A-18-16-30530) reported the OIG findings and recommendations as follows:

We conducted this audit because OIG had identified ensuring the safety and effectiveness of medical devices and fostering a culture of cybersecurity as top management challenges for HHS.

We also considered public and Congressional interest in medical device cybersecurity risks to patients and the Internet of Things. The Food and Drug Administration (FDA) is the HHS operating division responsible for assuring that legally marketed medical devices are safe and effective.

Our objective was to determine the effectiveness of FDA's plans and processes for timely communicating and addressing cybersecurity medical device compromises in the post market phase.

We focused this audit on FDA's internal processes for addressing the cybersecurity of medical devices in the post market phase. To accomplish our objective, we reviewed FDA's policies, procedures, manuals, and guides; interviewed staff; and reviewed publicly available information on FDA's website. We also analyzed FDA's processes for receiving and evaluating information on medical device compromises. In addition, we tested the internal controls at FDA's Center for Devices and Radiological Health to determine whether they ensured an effective response to a medical device cybersecurity incident.

FDA had plans and processes for addressing certain medical device problems in the post market phase, but its plans and processes were deficient for addressing medical device cybersecurity compromises. Specifically, FDA's policies and procedures were insufficient for handling post market medical device cybersecurity events; FDA had not adequately tested its ability to respond to emergencies resulting from cybersecurity events in medical devices; and, in 2 of 19 district offices, FDA had not established written standard operating procedures to address recalls of medical devices vulnerable to cyber threats.

These weaknesses existed because, at the time of our fieldwork, FDA had not sufficiently assessed medical device cybersecurity, an emerging risk to public health and to FDA's mission, as part of an enterprise risk management process. We shared our preliminary findings with FDA in advance of issuing our draft report. Before we issued our draft report, FDA implemented some of our recommendations. Accordingly, we kept our original findings in the report, but, in some instances, removed our recommendations.

We recommend that FDA do the following: (1) continually assess the cybersecurity risks to medical devices and update, as appropriate, its plans and strategies; (2) establish written procedures and practices for securely sharing sensitive information about cybersecurity events with key stakeholders who have a "need to know"; (3) enter into a formal agreement with Federal agency partners, namely the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team, establishing roles and responsibilities as well as the support those agencies will provide to further FDA's mission related to medical device cybersecurity; and (4) ensure the establishment and maintenance of procedures for handling recalls of medical devices vulnerable to cybersecurity threats.

FDA agreed with our recommendations and said it had already implemented many of them during the audit and would continue working to implement the recommendations in the report. However, FDA disagreed with our conclusions that it had not assessed medical device cybersecurity at an enterprise or component level and that its preexisting policies and

procedures were insufficient. We appreciate the efforts FDA has taken and plans to take in response to our findings and recommendations, but we maintain that our findings and recommendations are valid.

The HHS OIG, along with Federal and State law enforcement partners, participated in the largest ever prescription opioid law enforcement operation. The Appalachian Regional Prescription Opioid Surge Takedown resulted in charges against 60 individuals, including 53 medical professionals, for their alleged participation in the illegal prescribing and distributing of opioids and other dangerous narcotics and for healthcare fraud schemes. The charges involve over 350,000 prescriptions for controlled substances and over 32 million pills in West Virginia, Ohio, Kentucky, Alabama, and Tennessee. More than 24,000 patients in the region who received prescriptions from these medical professionals over the past 2 years are affected by the law enforcement activity. This effort demonstrates the positive impact the Medicare Fraud Strike Force is making in our communities.

The HHS OIG, with our law enforcement partners, announced in April 2019 our efforts in dismantling one of the largest healthcare fraud schemes ever investigated, in terms of amount billed to Medicare. Twenty-four defendants in 17 Federal districts were charged for allegedly participating in the scheme, in which fraudsters submitted over $1.7 billion in Medicare claims and were paid $900 million. In the alleged scheme, medical professionals working with fraudulent telemedicine companies received illegal kickbacks and bribes from medical equipment companies. In exchange, the medical equipment companies obtained prescriptions for medically unnecessary orthotic braces and used them to fraudulently bill Medicare. This enforcement action demonstrates the positive impact OIG is making to fight fraud and protect HHS programs and beneficiaries.

The Unaccompanied Alien Children program (UAC), operated by the Office of Refugee Resettlement (ORR) within the Administration for Children and Families (ACF), provides temporary housing, food, clothing, and other related services to unaccompanied minor children in its custody. In 2018, OIG announced that the agency would rapidly deploy multidisciplinary teams to conduct site visits at ORR-funded facilities nationwide to review the care and well-being of all children residing in these facilities, including the subset of children who were separated due to the zero-tolerance policy. As part of this body of work, OIG also reviewed HHS program data and interviewed HHS staff, officials, and senior leadership to understand how HHS identified and tracked separated children. In three weeks, more than 200 OIG staff completed multi-day site visits to 45 ORR-funded facilities across the country. A series of reports are being released as a result of the site visits.

The HHS OIG, along with our state and federal law enforcement partners, participated in the largest health care fraud takedown in history in June 2018. More than 600 defendants in 58 federal districts were charged with participating in fraud schemes involving about $2 billion in losses to Medicare and Medicaid. Since the last takedown, OIG also issued exclusion notices to 587 doctors, nurses, and other providers based on conduct related to opioid diversion and abuse. These enforcement actions protect Medicare and Medicaid and deter fraud -- sending a strong signal that theft from these taxpayer-funded programs will not be tolerated. The money taxpayers

spend fighting fraud is an excellent investment: For every $1 spent on health care-related fraud and abuse investigations in the last 3 years, more than $4 has been recovered.

U.S. Department of Justice OIG

The Office of the Inspector General (OIG) in the U.S. Department of Justice (DOJ) is a statutorily created independent entity whose mission is to detect and deter waste, fraud, abuse, and misconduct in DOJ programs and personnel, and to promote economy and efficiency in those programs. The OIG investigates alleged violations of criminal and civil laws by DOJ employees and also audits and inspects DOJ programs. The Inspector General, who is appointed by the President subject to Senate confirmation, reports to the Attorney General and Congress.

The Office of the Inspector General (OIG) consists of a front office, which is comprised of the Inspector General, the Deputy Inspector General, the Office of the General Counsel, and six major components. Each division is headed by an Assistant Inspector General. The OIG has a staff of approximately 500 employees, about half of whom are based in Washington, D.C., while the rest work from 17 Investigations Division field and area offices and 6 Audit Division regional offices located throughout the country.

The **Audit Division** is the OIG's largest division and is made up of 200 skilled auditors, program analysts, statisticians and other operational staff. Through its multi-disciplined staff, the Audit Division conducts performance audits of Department programs and operations and oversees annual audits of over $35 billion in Department expenditures. The Division also conducts audits of external entities that receive Department funding through its various contracts and grant programs. These audits significantly assist the Department in its efforts to prevent waste, fraud and abuse, and to promote economy and efficiency in its operations. The Division's robust oversight program is primarily driven by risk-based assessments of Department operations, as well as legal mandates, congressional requests, current events, and the Department's Top Management and Performance Challenges as identified by the OIG each year.

The Investigations Division investigates alleged violations of fraud, abuse and integrity laws that govern DOJ employees, operations, grantees and contractors. Investigations Division Special Agents develop cases for criminal prosecution, civil, or administrative action.

The Evaluation and Inspections Division provides the Inspector General with an alternative mechanism to traditional audit and investigative disciplines to assess Department of Justice (Department) programs and activities. Much of the work results in recommendations to decision makers to streamline operations, reduce unnecessary regulations, improve customer service, and minimize inefficient and ineffective procedures. In addition to assessing Department programs, the Division conducts special reviews requested by the Inspector General or senior Department management that arise suddenly and need immediate attention.

The Oversight and Review Division blends the skills of attorneys, investigators, program analysts, and paralegals to conduct special reviews and investigations of sensitive allegations involving Department employees and operations. O&R's reviews and investigations are often undertaken at the request of the Attorney General, senior Department managers, or Congress.

The Information Technology Division executes the OIG's IT strategic vision and goals by directing technology and business process integration, network administration, implementation

of computer hardware and software, cybersecurity, applications development, programming services, policy formulation, and other mission-support activities.

The Management and Planning Division provides the Inspector General with advice on administrative and fiscal policy and assists OIG components by providing services in the areas of planning, budget, finance, quality assurance, personnel, communications, procurement, facilities, telecommunications, security, and general support.

Top Management Challenges of DOJ have been:

2018 Challenges:

- Advancing National Security, Protecting Sensitive Information, and Safeguarding Civil Liberties
- Enhancing Cybersecurity with Emerging Technology and Collaboration
- Managing an Overcrowded Federal Prison System in an Era of Declining Resources
- Building Productive Relationships and Trust Between Law Enforcement and Communities
- Coordinating within the Department and Across Government to Fulfill the Department's Mission to Combat Crime
- Administering and Overseeing Contracts and Grants
- Effectively Applying Performance-Based Management to Inform Decision Making and Improve Outcomes
- Filling Mission Critical Positions Despite Department Challenges and Delays in the Onboarding Process
- Ensuring Adherence to Established Department Policies and Procedures

2017 Challenges:

- Safeguarding National Security and Ensuring Privacy and Civil Liberties Protections
- Enhancing Cybersecurity in an Era of Increasing Threats
- Managing an Overcrowded Federal Prison System in an Era of Declining Resources
- Strengthening the Relationships Between Law Enforcement and Local Communities and Promoting Public Trust
- Coordinating within the Department and Across Government to Fulfill the Department's Mission to Combat Crime
- Administering and Overseeing Contracts and Grants
- Using Performance-Based Management To Improve Department Programs
- Filling Mission Critical Positions Despite Competition for Highly-Skilled Professionals and Delays in the Onboarding Process

Ongoing Work of DOJ OIG includes:

Administration of Joint Law Enforcement Operations Funds

The OIG is conducting an audit of the USMS's administration of Joint Law Enforcement Operations (JLEO) funds. Our preliminary objectives are to determine if the USMS: (1) has

proper controls for JLEO funds reimbursement, and (2) reimburses State and local law enforcement for allowable and supported costs.

Assessment of and Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015

The Inspectors General of the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and Treasury, and the Intelligence Community, are assessing the actions taken over the prior, most recent, 2-year period to carry out the requirements of the Cybersecurity Information Sharing Act of 2015 (CISA). The Inspectors General, in consultation with the Council of Inspectors General on Financial Oversight, will jointly submit an interagency report to Congress. The objective of this project is to assess the actions taken to carry out CISA requirements during calendar years 2017 and 2018 and submit an unclassified, interagency report to Congress by December 2019. The information obtained from the Department will be provided to the IC IG for the joint report.

ATF Contracts Awarded to Shearwater Systems, LLC, to Support Violent Gun Crime Reduction Intelligence Initiatives

The OIG is auditing the ATF's contracts awarded to Shearwater Systems, LLC (Shearwater), to support violent gun crime reduction intelligence initiatives. The preliminary audit objectives are to assess: (1) ATF's acquisition planning, administration, and oversight of the contracts and task orders; and (2) Shearwater's performance and compliance with the contracts' and task orders' terms and conditions, including financial management, monitoring, reporting, and progress toward meeting the contract goals and objectives, as well as applicable laws and regulations.

Audit of DOJ's Efforts to Protect BOP Facilities Against Threats Posed by Unmanned Aircraft Systems

The OIG is auditing the Department's efforts to protect BOP facilities against threats posed by unmanned aircraft systems, commonly referred to as drones. The preliminary objectives are to: (1) determine the extent to which the BOP can detect and track attempts to deliver contraband to BOP facilities via drones, and (2) assess the Department's current policies and efforts to protect BOP facilities against security threats posed by drones.

Audit of FBI's Regional Computer Forensic Laboratory – Western New York

The OIG is conducting an audit of the Western New York Regional Computer Forensic Laboratory (WNYRCFL) located in Buffalo, New York. The objectives of the audit are to assess: (1) the efficiency and effectiveness of the WNYRCFL's performance; (2) the effectiveness of the WNYRCFL's outreach and partnership with the law enforcement community; and (3) the WNYRCFL's case management system and its efforts to address its service backlog.

Audit of the Drug Enforcement Administration's Community-Based Efforts to Combat the Opioid Crisis

The OIG is conducting an audit of the DEA's community-based efforts to combat the opioid crisis. The preliminary objectives are to: (1) examine the DEA's pilot city-selection methodology, (2) assess the DEA's integration of a performance measurement strategy to enhance its community-based efforts, (3) evaluate the DEA's collaboration with other agencies in combatting the opioid crisis, and (4) assess the DEA's efforts to sustain progress in the communities it assists.

Audit of the Executive Office for Immigration Review's Financial Management Practices

The OIG initiated an audit of the Executive Office for Immigration Review's (EOIR) financial management practices. The preliminary objective is to assess EOIR's efforts to identify effectively its funding needs and execute its budget.

Audit of the FBI's Intermountain West Regional Computer Forensic Laboratory

The OIG initiated an audit of the Intermountain West Regional Computer Forensic Laboratory (IWRCFL) located in Salt Lake City, Utah, with satellite laboratories in Billings, Montana, and Boise, Idaho. The objectives of the audit are to assess: (1) the efficiency and effectiveness of the IWRCFL's laboratory performance; (2) the effectiveness of the IWRCFL's outreach and partnership with the law enforcement community; and (3) the IWRCFL's case management system and its efforts to address its service request backlog.

Audit of the Federal Bureau of Investigation Child Pornography Victim Assistance Program

The OIG initiated an audit of the FBI Child Pornography Victim Assistance Program. The objectives of the audit are to (1) evaluate the FBI's process for obtaining images of victimization, (2) evaluate the FBI's process for notifying victims of child pornography and their guardians, and (3) determine whether the FBI appropriately secured personally identifiable information pertaining to program operations.

Audit of the Superfund Activities in the Environment and Natural Resources Division for Fiscal Years 2017 and 2018

The OIG is conducting an audit of the fiscal years (FY) 2017 and 2018 Superfund activities relating to the costs incurred by the Environment and Natural Resources Division (ENRD) in litigating Superfund cases. The objective of the audit is to determine if the ENRD provided an equitable distribution of total labor costs, other direct costs, and indirect costs to Superfund cases during FYs 2017 and 2018.

Audits of the U.S. Department of Justice and Select Components Annual Financial Statements Fiscal Year 2019

The OIG is auditing DOJ and select components Annual Financial Statements for fiscal year 2019. Pursuant to Section 304(a) of the Chief Financial Officers Act of 1990, as expanded by Section 405(b) of the Government Management Reform Act of 1994, the OIG is required to perform an audit of the Department's annual financial statements. Additionally, the Civil Asset Forfeiture Reform Act of 2000 requires an audit of the Assets Forfeiture Fund/Seized Asset Deposit Fund annual financial statements, and the Government Corporation Control Act of 1945, as amended, requires an audit of the Federal Prison Industries, Inc. annual financial statements. The OIG has contracted with the independent public accounting firm, KPMG LLP, to perform the audits.

Audit of the U.S. Marshals Service's Awarding and Administration of Sole-Source Contracts

The OIG initiated an audit with the objective of evaluating the U.S. Marshals Service's awarding and administration of sole-source contracts.

BOP Counterterrorism Efforts

The OIG is conducting an audit of the BOP's counterterrorism efforts. The preliminary objectives are to review the BOP's policies, procedures, and practices for monitoring

communications of inmates with known or suspected ties to domestic and foreign terrorism and its efforts to prevent further radicalization among its inmate population.

BOP Non-Lethal/Lethal Fence System Updates and Improvements Contract Awarded to DeTekion Security Systems, Inc.

The OIG is conducting an audit of the BOP's contract awarded to DeTekion Security Systems, Inc., and the related initial contract actions to install non-lethal/lethal fence systems at nine United States Penitentiaries (USP). A non-lethal/lethal electrified fence has the capacity to administer a non-lethal shock to initially stun someone touching the fence and then switch to deliver a lethal shock if that person touches the fence a second time. The objectives are to: (1) evaluate BOP and contractor efforts on the design of the non-lethal/lethal fences installed at the nine USPs during the initial and current contract actions, (2) evaluate BOP's price analysis of the fence upgrade contract, (3) assess BOP's oversight of the fence upgrade contract, and (4) to evaluate BOP perimeter security strategy incorporated at the nine USPs that have DeTekion lethal/non-lethal fences.

BOP's Efforts to Address Inmate Sexual Harassment and Sexual Assault Against BOP Staff

The OIG is conducting a review of the BOP's efforts to address inmate-on-staff sexual misconduct. The review will assess the prevalence and impacts of inmate-on-staff sexual misconduct, including sexual harassment, assault, and abuse, in BOP institutions from fiscal year (FY) 2008 through FY 2018.

Contract Awarded to Correct Care Solutions, LLC for the Federal Correctional Complex in Coleman, Florida

The OIG is auditing a BOP contract awarded to Correct Care Solutions, LLC. The objectives of the audit are to assess the BOP's award and administration of the contract, and Correct Care Solutions, LLC's performance and compliance with the terms, conditions, laws, and regulations applicable to this contract in the areas of: (1) contractor performance; (2) billings and payments; and (3) contract management, oversight, and monitoring.

Contract Awarded to the GEO Group, Incorporated to Operate the Robert A. Deyton Detention Center, Lovejoy, Georgia

The OIG initiated an audit of the USMS's contract awarded to the GEO Group, Incorporated. The preliminary objective of the audit is to assess the USMS's administration of the contract, and the GEO Group, Incorporated's performance and compliance with the terms, conditions, laws, and regulations applicable to this contract. The assessment of performance may include financial management, monitoring, reporting, and progress toward meeting the contract goals and objectives.

DEA's Controls over Weapons, Munitions, and Explosives

The OIG is auditing DEA's controls over weapons, munitions, and explosives, including firearms, Tasers, ammunition, less-lethal munitions, and diversionary devices. The preliminary objectives are to evaluate: (1) DEA's controls over weapons, munitions, and explosives; (2) DEA's compliance with policies governing weapons, munitions, and explosives; and (3) the accuracy of DEA's weapons, munitions, and explosives inventories.

DEA's Income-Generating Undercover Operations

The OIG is conducting an audit of the DEA's income-generating undercover operations. The preliminary objectives are to evaluate the management and oversight of DEA's income-generating operations with respect to: (1) the initiation and classification of these operations, (2) the controls over and use of funds during operations, and (3) the disposal of proceeds at the conclusion of these operations.

DEA's Prescription Drug Take Back Activities

The OIG is auditing DEA's prescription drug take back activities. The preliminary objective is to evaluate the DEA's policies, procedures, and practices for the collection, custody, and disposal of prescription drugs.

DOJ's Compliance with the Federal Funding Accountability and Transparency Act of 2006, as amended by the DATA Act of 2014

The OIG is examining DOJ's compliance with reporting requirements under the Federal Funding Accountability and Transparency Act, as amended by the DATA Act. Through memorandum M-15-12, Increasing Transparency of Federal Spending by Making Federal Spending Data Accessible, Searchable, and Reliable, the Office of Management and Budget provided guidance to federal agencies on the requirements that agencies must employ pursuant to the DATA Act. The OIG will review a statistically valid sampling of the fiscal year 2019 spending data submitted, and submit to Congress and make publicly available a report assessing the completeness, timeliness, quality, and accuracy of the data sampled.

Efforts to Address Challenges in Administering the Crime Victims Fund Programs

The OIG is reviewing the Office of Justice Programs' efforts to address challenges in administering the Crime Victims Fund (CVF) programs. The review is expected to include (1) assessing systemic issues facing CVF grant administration and (2) evaluating actions OJP has taken to ameliorate programmatic issues identified through OIG work.

Efforts to Address Homegrown Violent Extremists

The OIG is auditing the FBI's efforts to address homegrown violent extremists (HVE). The preliminary objectives are to: review the FBI's HVE casework and resource management; evaluate the FBI's coordination with relevant components and its strategic and tactical policies and processes to identify and assess HVE threats; and evaluate the FBI field divisions' implementation of strategic and tactical policies and processes to assess HVE threats.

Examination of the Department's and the FBI's Compliance with Legal Requirements and Policies in Applications Filed with the U.S. Foreign Intelligence Surveillance Court Relating to a certain U.S. Person

The OIG, in response to requests from the Attorney General and Members of Congress, is examining the Department's and the FBI's compliance with legal requirements, and with applicable DOJ and FBI policies and procedures, in applications filed with the U.S. Foreign Intelligence Surveillance Court (FISC) relating to a certain U.S. person. As part of this examination, the OIG is also reviewing information that was known to the DOJ and the FBI at the time the applications were filed from or about an alleged FBI confidential source. Additionally, the OIG is reviewing the DOJ's and FBI's relationship and communications with

the alleged source as they relate to the FISC applications. If circumstances warrant, the OIG will consider including other issues that may arise during the course of the review.

Executive Office for Immigration Review Recognition and Accreditation Program

The OIG initiated an audit of the Executive Office for Immigration Review (EOIR) Recognition and Accreditation Program. The preliminary objectives are to determine whether EOIR: (1) established effective controls for the selection, vetting, and certification of accredited representatives under the program; (2) monitors the activities of accredited representatives; and (3) established adequate procedures for investigating and resolving allegations of misconduct against accredited representatives.

FBI's Adjudication of Misconduct Investigations

The OIG is examining whether FBI's misconduct investigations are handled according to policy throughout the adjudication process and how FBI determines when and how to revise its misconduct adjudication policies and process.

FBI's Confidential Human Source Program

The OIG is auditing the FBI's Confidential Human Source Program. The preliminary objectives are to: (1) assess the FBI's management and oversight of its Confidential Human Source Program, to include the FBI's oversight of payments to confidential human sources, (2) examine the FBI's confidential human source policies to ensure consistency with the Attorney General Guidelines, and (3) assess the FBI's process of determining reliability and appropriateness of confidential human sources.

FBI Contract Awarded to Tuva, LLC

The OIG is conducting an audit of the FBI's contract awarded to Tuva, LLC. The preliminary objective of the audit is to assess the FBI's administration of the contract, and Tuva, LLC's performance and compliance with the terms, conditions, laws, and regulations applicable to this contract. The assessment of performance may include financial management, monitoring, reporting, and progress toward meeting the contract's goals and objectives.

FBI's Covert Contracts

The OIG is auditing the FBI's contracts awarded for covert activity. The preliminary objectives of the audit are to assess the FBI's awarding and administration of these covert contracts and to evaluate the FBI's procedures and processes for ensuring contractor performance and compliance with the terms, conditions, laws, and regulations applicable to these contracts.

FBI's National Security Undercover Operations

The OIG is conducting an audit of the FBI's National Security Undercover Operations. The preliminary objectives are to evaluate: (1) the FBI's oversight of national security-related undercover operations, and (2) the FBI's efforts to recruit and train agents for these undercover operations.

FBI's Strategy and Efforts to Disrupt Illegal Dark Web Activities

The OIG is auditing the FBI's strategy and efforts to disrupt illegal dark web activities. The preliminary objective is to assess the implementation of the FBI's dark web strategy.

Fiscal Year 2018 – Annual Information Technology Security Evaluation Pursuant to the Federal Information Security Management Act of 2014

The OIG is conducting the annual Federal Information Security Modernization Act of 2014 (FISMA) evaluation for fiscal year (FY) 2018. The OIG will use independent certified public accounting firms, under its direction, to evaluate the specific requirements of the Office of Management and Budget's FY 2018 guidelines and to complete the Department of Homeland Security's FY 2018 Reporting Metrics. FISMA requires that the OIG, or independent evaluators selected by the OIG, perform an annual independent evaluation of DOJ's security programs and practices.

Fiscal Year 2019 - Annual Information Technology Security Evaluation Pursuant to the Federal Information Security Modernization Act

The OIG initiated its annual Federal Information Security Modernization Act (FISMA) evaluation for FY 2019. The OIG will use an independent certified public accounting firm, under its direction, to evaluate the specific requirements of the Office of Management and Budget's FY 2019 guidelines and to complete the Department of Homeland Security's FY 2019 Reporting Metrics. FISMA requires that the OIG, or independent evaluators selected by the OIG, perform an annual independent evaluation of the Department's information security programs and practices.

Inspection and Review of MDC Brooklyn Facilities Issues and Related Impacts on Prisoners

The OIG is conducting an inspection and review of BOP's management of the electrical and heating issues that occurred beginning in January 2019 at the Metropolitan Detention Center Brooklyn. The OIG will assess how those issues occurred, whether BOP has in place adequate contingency plans for such an incident, and how they affected prisoners' conditions of confinement and access to counsel. The OIG will also assess steps BOP management officials took to address and resolve those issues. If circumstances warrant, the OIG will consider including other issues that may arise during the course of the inspection and review.

Management of the Justice Prisoner and Alien Transportation System

The OIG is conducting an audit of USMS's management of the Justice Prisoner and Alien Transportation System (JPATS). The preliminary objective of the audit will be to evaluate USMS's efforts to achieve its strategic goal of improving the effectiveness and efficiency of JPATS prisoner and detainee transportation.

OJP Corrective Actions to Resolve and Close Audit Reports during FYs 2015 through 2017

The OIG is auditing the Office of Justice Programs' (OJP) corrective actions to resolve and close audit reports during FYs 2015 through 2017. The preliminary objective is to assess and summarize the corrective actions taken by OJP to close OIG audit recommendations issued in audit reports that were closed during FYs 2015 through 2017.

Review of Cooperation between the Departments of Justice and Homeland Security in Southwest Border Criminal Investigations

The Inspectors General of the U.S. Departments of Justice and Homeland Security (DHS) are jointly reviewing cooperation primarily between the FBI, DHS' Homeland Security Investigations (HSI), and the U.S. Attorney's Offices on criminal investigations along the U.S. Southwest border. This review will focus on deconflicting investigations and operations, as well

as sharing information on investigations conducted by the FBI and HSI and prosecuted by U.S. Attorney's Offices.

Review of the Department of Justice's Preparedness to Respond to Critical Incidents Under Emergency Support Function 13

The OIG is reviewing the Department's ability to meet its responsibilities under Emergency Support Function 13 (ESF-13) and to execute ESF-13 activities in response to natural and manmade disasters. OIG will assess Departmental policies and guidance; planning, preparation, training, and execution processes; and coordination among DOJ law enforcement components and non-DOJ support agencies in support of an ESF-13 activation.

Review of the Department's Planning and Implementation of Its Zero Tolerance Policy and its Coordination with the Departments of Homeland Security and Health and Human Services

The OIG is reviewing DOJ's planning and implementation of its zero tolerance policy relating to prosecution of persons for entering the United States illegally in southwest border jurisdictions. The review also will assess the Department's coordination with the Departments of Homeland Security and Health and Human Services on the policy's implementation. Consistent with the Inspector General Act and the OIG's role, the review will not substitute the OIG's judgment for the judgments made by the Department regarding the substantive merits of the policy.

Review of the Department's Violent Crime Initiatives

The OIG is reviewing the Department's strategic planning and accountability measures for combatting violent crime, including coordination across Department prosecution, law enforcement, and grant making components; and strategic planning for providing assistance to communities that are confronting significant increases in homicides and gun violence.

Review of the Drug Enforcement Administration's Opioid Enforcement Efforts

The OIG is assessing whether DEA's regulatory activities and enforcement efforts effectively prevent the diversion of controlled substances, particularly opioids, to unauthorized users. Specifically, this review will examine (1) DEA's enforcement regulations, policies, and procedures; (2) DEA's use of enforcement actions involving manufacturers, distributors, physicians, and pharmacists who violate these policies and procedures; and (3) DEA's coordination with state and local partners to combat the opioid epidemic.

Review of the Federal Bureau of Prisons' Pharmaceutical Drug Costs for Inmates

The OIG is conducting a review of the BOP's pharmaceutical drug costs for inmates. This review will examine the BOP's drug rates and spending, its drug procurement process, and its effort to control rising drug costs. Included in this review is a more specific evaluation of the BOP's management of Hepatitis C.

Review of the Institutional Hearing and Removal Program

The OIG is reviewing the actions taken by the Department of Justice (Department), including the Executive Office for Immigration Review and Federal Bureau of Prisons, to expand the Institutional Hearing and Removal Program (IHRP). The review will assess the steps the Department took to expand the number of IHRP sites, enhance video teleconferencing capabilities, and coordinate with the Department of Homeland Security.

Review of the U.S. Marshals Service's Pharmaceutical Drug Costs for Detainees

The OIG is conducting a review of the USMS's pharmaceutical drug costs for detainees. This review will examine the USMS's process for and spending on drug procurement under the National Managed Care Contract, as well as its efforts to control rising drug costs.

Review of the U.S. Marshals Service's Tactical Training Officer Program

The OIG is examining the U.S. Marshals Service's (USMS) Tactical Training Officer (TTO) Program that it established in 2011. The review will cover the TTO Program's policies, procedures, and training provided to USMS personnel and Task Force Officers. The review will also focus on how the TTO Program has changed USMS training and operations for conducting high-risk fugitive apprehensions.

Major reports released by DOJ OIG in 2019 include:
Procedural Reform Recommendation for the Department of Justice June 12, 2019
Report on the Department of Justice's Use of Immigration Sponsorship Programs May 22, 2019
Report on the Bureau of Alcohol, Tobacco, Firearms and Explosives' Controls over Agent Cashier Funds April 1, 2019
Report on the FBI's Cyber Victim Notification Process March 28, 2019
Report on the Drug Enforcement Administration's Use of Administrative Subpoenas to Collect or Exploit Bulk Data March 21, 2019
Report on the Federal Bureau of Prisons' Perimeter Security Upgrade Contract for Administrative U.S. Penitentiary Thomson Awarded to DeTekion Security Systems, Inc. March 21, 2019
Report on the FBI's Management of Maritime Terrorism Threats March 14, 2019
Report on the Bureau of Alcohol, Tobacco, Firearms and Explosives Sole-Source Small Business Contracting March 14, 2019
Report on Efforts to Safeguard Minors in DOJ Youth-Centered Programs March 12, 2019
Report on the Federal Bureau of Investigation's Oversight and Administration of the National Vehicle Lease Program and its Contract with EAN Holdings, LLC February 28, 2019
Audit of the National Institute of Justice's Grants Management February 14, 2019
Report on the Office on Violence Against Women Training and Technical Assistance Program February 14, 2019
Report on the Bureau of Alcohol, Tobacco, Firearms and Explosives' Implementation of the Frontline Initiative February 13, 2019
Procedural Reform Recommendation for the USMS Concerning the Imposition of Prompt and Effective Discipline for Employee Misconduct February 12, 2019
Procedural Reform Recommendation for the FBI Concerning the Collection and Retention of Text Messages Sent To or From FBI-Issued Mobile Devices Updated: July 2019

U.S. Department of Homeland Security OIG

Both the Department of Homeland Security (DHS) Act and this Office of Inspector General (OIG) were established by Congress in 2002. The OIG is led by an Inspector General who is appointed by the President and subject to Senate confirmation. The vision of DHS OIG is to drive transformative change to improve DHS programs and operations and promote a safer homeland by providing independent oversight and promote excellence, integrity, and accountability within DHS. The OIG focuses its oversight on DHS' core mission areas:

- Preventing Terrorism and Enhancing Security;
- Securing and Managing Our Borders;
- Enforcing and Administering Our Immigration Laws;
- Safeguarding and Securing Cyberspace;
- Ensuring Resilient Response to Disasters

Fiscal Year 2018 OIG Accomplishments:

Dollar Impact:
Questioned Costs: $175,133,425
Funds Put to Better Use: $77,657,165
Funds Recovered / Deobligated: $58,748,471
Restitution: $27,561,639
Fines: $60,491
Asset Forfeiture: $72,947,509

Activities:
Reports Issued: 89
Recommendations Issued: 318
Recommendations Closed: 279
Hotline Complaints Received: 40,657
Whistleblower Complaints Received: 198
Investigations Referred to Prosecution: 202
Investigations Closed: 856
Arrests: 103
Convictions: 76
Indictments: 133

Major Reports by DHS OIG in 2019	Date
CBP's Global Entry Program Is Vulnerable to Exploitation	06/24/2019
DHS Needs to Improve Its Oversight of Misconduct and Discipline	06/17/2019
Concerns about ICE Detainee Treatment and Care at Four Detention Facilities	06/03/2019
Management Alert - DHS Needs to Address Dangerous Overcrowding Among	05/30/2019

Single Adults at El Paso Del Norte Processing Center	
Lessons Learned from Prior Reports on FEMA's 50 Percent Repair-or-Replace Rule Decisions	05/29/2019
Audit of DHS' Issuance and Management of Other Transaction Agreements Involving Consortium Activities	05/30/2019
Department of Homeland Security's FY 2018 Compliance with the Improper Payments Elimination and Recovery Act of 2010 and Executive Order 13520, Reducing Improper Payments	05/24/2019
DHS Needs to Address Oversight and Program Deficiencies before Expanding the Insider Threat Program	05/24/2019
Special Report: Review Regarding DHS OIG's Retraction of Thirteen Reports Evaluating FEMA's Initial Response to Disasters	05/22/2019
Data Quality Improvements Needed to Track Adjudicative Decisions	05/14/2019
Audit of Department of Homeland Security's Fiscal Year 2017 Conference Spending	05/22/2019
FEMA Should Not Have Awarded Two Contracts to Bronze Star LLC	05/07/2019
Additional Controls Needed to Better Manage FEMA's Transitional Sheltering Assistance Program	04/02/2019
Missouri's Management of State Homeland Security Program and Urban Areas Security Initiative Grants Awarded During Fiscal Years 2012 through 2015	03/29/2019
TSA Needs to Improve Efforts to Retain, Hire, and Train Its Transportation Security Officers	03/28/2019
(U) Evaluation of DHS' Compliance with Federal Information Security Modernization Act Requirements for Intelligence Systems for Fiscal Year 2018	03/21/2019
Review of U.S. Coast Guard's Fiscal Year 2018 Detailed Accounting Submission for Drug Control Funds	03/18/2019
Management Alert - FEMA Did Not Safeguard Disaster Survivors' Sensitive Personally Identifiable Information (REDACTED)	03/15/2019
Oregon's Management of State Homeland Security Program and Urban Areas Security Initiative Grants Awarded During Fiscal Years 2013 through 2015	03/13/2019
Review of U.S. Immigration and Customs Enforcement's Fiscal Year 2018 Drug	03/08/2019

Control Performance Summary Report	
Review of U.S. Customs and Border Protection's Fiscal Year 2018 Detailed Accounting Submission for Drug Control Funds	03/08/2019
ICE Faces Barriers in Timely Repatriation of Detained Aliens	03/11/2019
Review of U.S. Coast Guard's Fiscal Year 2018 Drug Control Performance Summary Report	03/08/2019
Review of U.S. Customs and Border Protection's Fiscal Year 2018 Drug Control Performance Summary Report	03/08/2019
Review of U.S. Immigration and Customs Enforcement's Fiscal Year 2018 Detailed Accounting Submission for Drug Control Funds	03/07/2019
Progress Made, But Additional Efforts are Needed to Secure the Election Infrastructure	02/28/2019
Border Patrol Needs a Staffing Model to Better Plan for Hiring More Agents	02/28/2019
United States Coast Guard's Reporting of Uniform Code of Military Justice Violations to the Federal Bureau of Investigation	02/21/2019
Covert Testing of Access Controls to Secure Airport Areas	02/13/2019
Issues Requiring Action at the Essex County Correctional Facility in Newark, New Jersey	02/13/2019
DHS Needs to Improve the Process for Identifying Acquisition Planning Capability Needs	01/30/2019
ICE Does Not Fully Use Contracting Tools to Hold Detention Facility Contractors Accountable for Failing to Meet Performance Standards	01/29/2019
FAMS' Contribution to International Flight Security is Questionable	12/19/2018
DHS' and TSA's Compliance with Public Law 114-278, Transportation Security Card Program Assessment	12/14/2018
The Federal Protective Service Has Not Managed Overtime Effectively	12/11/2018
Oversight Review of the Department of Homeland Security Immigration and Customs Enforcement, Office of Professional Responsibility, Investigations Division	12/06/2018
Management Alert - CBP Needs to Address Serious Performance Issues on the	12/06/2018

Accenture Hiring Contract	
FEMA Should Recover $3,061,819 in Grant Funds Awarded to Jackson County, Florida	12/04/2018
CBP Did Not Maximize its Revenue Collection Efforts for Delinquent Debt Owed from Importers	12/04/2018
CBP's Searches of Electronic Devices at Ports of Entry	12/03/2018
FEMA Should Recover $413,074 of Public Assistance Grant Funds Awarded to Nashville-Davidson County, Tennessee, for a May 2010 Flood	11/29/2018
FEMA's Oversight of the Integrated Public Alert & Warning System (IPAWS)	11/19/2018
DHS Training Needs for Hiring 15,000 Border Patrol Agents and Immigration Officers	11/20/2018
FEMA Should Disallow $22.3 Million in Grant Funds Awarded to the Chippewa Cree Tribe of the Rocky Boy's Indian Reservation, Montana	11/28/2018
FEMA Should Disallow $9.1 Million in Public Assistance Grant Funds Awarded to Ascension Parish School Board, Louisiana	11/16/2018
Independent Auditors' Report on DHS' FY 2018 Financial Statements and Internal Control over Financial Reporting	11/15/2018
Management Alert - Coast Guard Investigative Service Search and Seizure of DHS OIG and Congressional Communications	10/29/2018
CBP Should Improve Its Air Coordination of the Rio Grande Valley Sector	10/18/2018
Major Management and Performance Challenges Facing the Department of Homeland Security	11/09/2018
(U) S&T Has Taken Steps to Address Insider Threats, But Management Challenges Remain	09/28/2018

In 2019 the OIG found that DHS does not have sufficient policies and procedures to address employee misconduct. Specifically, the Department's policy does not include procedures for reporting allegations of misconduct, clear and specific supervisor roles and expectations, or clearly defined key discipline terms. These deficiencies occurred because DHS' Employee Relations office has limited staff, who do not believe they are responsible for managing the allegation process. DHS also does not effectively manage the misconduct program throughout the Department, lacking data monitoring and metrics to gauge program performance. Without oversight through defined policies and program management, DHS cannot make informed

decisions to improve the program and ensure all components manage the misconduct process consistently. Additionally, this shortcoming could lead to costly litigation due to inappropriate or unenforceable disciplinary determinations.

In addition, the OIG also reported that overall, our inspections of four detention facilities revealed violations of ICE's 2011 Performance-Based National Detention Standards, which set requirements for facilities housing detainees. This report summarizes findings on our latest round of unannounced inspections at four detention facilities housing ICE detainees. Although the conditions varied among the facilities and not every problem was present at each, our observations, detainee and staff interviews, and document reviews revealed several common issues. Because we observed immediate risks or egregious violations of detention standards at facilities in Adelanto, CA, and Essex County, NJ, including nooses in detainee cells, overly restrictive segregation, inadequate medical care, unreported security incidents, and significant food safety issues, we issued individual reports to ICE after our visits to these two facilities. All four facilities had issues with expired food, which puts detainees at risk for food-borne illnesses. At three facilities, we found that segregation practices violated standards and infringed on detainee rights. Two facilities failed to provide recreation outside detainee housing units. Bathrooms in two facilities' detainee housing units were dilapidated and moldy. At one facility, detainees were not provided appropriate clothing and hygiene items to ensure they could properly care for themselves. Lastly, one facility allowed only non-contact visits, despite being able to accommodate in-person visitation. Our observations confirmed concerns identified in detainee grievances, which indicated unsafe and unhealthy conditions to varying degrees at all of the facilities we visited.

In another report the OIG stated that the Department of Homeland Security has taken some steps to mitigate risks to the Nation's election infrastructure; however, improved planning, more staff, and clearer guidance could facilitate its coordination with states. Specifically, despite Federal requirements, DHS has not completed the plans and strategies critical to identifying emerging threats and mitigation activities, and establishing metrics to measure progress in securing the election infrastructure. Senior leadership turnover and a lack of guidance and administrative staff have hindered DHS' ability to accomplish such planning. Until such issues are addressed and resolved, DHS cannot ensure effective guidance, unity of effort, and a well-coordinated approach to securing the Nation's election infrastructure.

Further, DHS provides assistance to state and local election officials upon request. Over time, the assistance provided has increased and the quality of information shared has improved. However, staff shortages, a lengthy security clearance process, and state and local officials' historic mistrust of Federal government assistance restrict DHS' efforts to provide the services and assessments needed to secure the election infrastructure. Addressing these issues is essential for continued improvement in the services, outreach, and quality of information DHS shares with election stakeholders.

U.S. Department of Defense OIG

The mission of the DoD OIG is to detect and deter fraud, waste, and abuse in Department of Defense programs and operations; promote the economy, efficiency, and effectiveness of the DoD; and help ensure ethical conduct throughout the DoD.

The DoD OIG's headquarters is located in Alexandria, Virginia. The OIG also has more than 50 field offices located in the United States, Europe, Southwest Asia, and South Korea. Over 1,000 DoD OIG employees are assigned to OIG headquarters, and more than 500 OIG employees, mostly auditors and investigators, are assigned to DoD OIG field offices. At any time, approximately 50 employees are temporarily assigned in Southwest Asia. DoD OIG programs are:

- Civil Liberties Program
- Contractor Disclosure Program
- DoD Joint Inspector General Program
- Equal Employment Opportunity Program
- Privacy Program
- Single Audit Program
- Subpoena Program

The DoD OIG identified these challenges based on a variety of factors, including DoD OIG oversight work, research, and judgment; oversight work done by other DoD Components; oversight work conducted by the Government Accountability Office; and input from DoD officials. While the DoD OIG reviewed DoD statements, documents, and assessments of these and other critical issues, the DoD OIG identified these top challenges independently.

The top management challenges document discusses each challenge, actions taken by the DoD to address the challenge, and oversight work by the DoD OIG and others related to the challenge. As reflected in this document, the FY 2019 top 10 DoD management and performance challenges are:

1. Implementing DoD Reform Initiatives
2. Countering China, Russia, Iran, and North Korea
3. Countering Global Terrorism
4. Financial Management: Implementing Timely and Effective Actions to Address Financial Management Weaknesses Identified During the First DoD-Wide Financial Statement Audit
5. Improving Cyber Security and Cyber Capabilities
6. Ensuring Ethical Conduct
7. Enhancing Space-Based Operations, Missile Detection and Response, and Nuclear Deterrence
8. Improving Readiness Throughout the DoD
9. Acquisition and Contract Management: Ensuring that the DoD Gets What It Pays For On Time, at a Fair Price, and With the Right Capabilities
10. Providing Comprehensive and Cost-Effective Health Care

Examples of criminal investigation and prosecution results resulting from DoD OIG actions:

June 24, 2019 Two Physicians and Two Registered Nurses Indicted in Mississippi Compounding Pharmacy Fraud Scheme. Two Mississippi-licensed physicians and two Mississippi-licensed registered nurses were charged in an indictment unsealed today for their roles in a multimillion dollar scheme to defraud TRICARE, the health care benefit program serving U.S. military, veterans and their respective family members, as well as private health care benefit programs Blue Cross & Blue Shield of Mississippi and United Healthcare of Mississippi.

June 17, 2019 Granite Bay Man Sentenced For Multi-Million Dollar Product Substitution Fraud On Federal Government Agencies. U.S. District Judge Kimberly J. Mueller sentenced Jim A. Meron, 54, of Granite Bay, today to 33 months in prison and three years of supervised release on two counts of wire fraud arising out of a government-procurement fraud scheme, U.S. Attorney McGregor W. Scott announced. As part of the sentence, the Court ordered Meron to pay restitution of $1,622,729.13 to dozens of victims. The Court also entered a final order forfeiting more than $1.7 million in assets seized during the investigation of Meron's crimes.

June 14, 2019 United States Files False Claims Act Complaint Against Two Compounding Pharmacies and Their Owner For Submitting Inflated Claims and Improperly Waiving Patient Copayments. The Department of Justice announced today that the United States has filed a complaint in intervention against Smart Pharmacy Inc., and SP2 LLC, two compounding pharmacies located in Jacksonville, Florida. The complaint alleges that the pharmacies improperly included the drug aripiprazole, an atypical antipsychotic drug, in compounded pain creams in order to boost the pharmacies' reimbursement for the prescriptions and that the pharmacies routinely waived patient copayment obligations. The government has also brought claims against Gregory Balotin, a co-owner of the pharmacies, for his involvement in the alleged schemes.

June 13, 2019 Three Physicians and Five Marketers Charged for Violations to Federal Anti-Kickback Statutes. Three physicians and five marketers have been charged in U.S. District Court with violations of the federal anti-kickback statute and other criminal offenses, announced U.S. Attorney Trent Shores. The men allegedly caused federal health care insurance programs to pay reimbursement costs for fraudulent and expensive compounding drug prescriptions written by recruited doctors in return for kickback payments. The defendants would then use the reimbursed funds for their own financial gain.

June 13, 2019 "Wholesaler Admits to Conspiracy to Manufacture and Sell Counterfeit Goods to the U.S. Military & Government. A Brooklyn, N.Y., clothing and goods wholesaler pleaded guilty in U.S. District Court in Providence today to charges related to his participation in a conspiracy that sold more than twenty million dollars worth of Chinese-made counterfeit goods to the United States military, government purchasers, and companies that supply the U.S. Government.

June 11, 2019 Medical Device Maker ACell, Inc. Pleads Guilty And Will Pay $15 Million To Resolve Criminal Charges And Civil False Claims Allegations. ACell, Inc. (ACell), a Maryland-

based medical device manufacturer, pleaded guilty to charges relating to its MicroMatrix powder wound-dressing product (MicroMatrix). ACell entered a guilty plea before U.S. District Court Judge Ellen L. Hollander in the District of Maryland to one misdemeanor count of failure and refusal to report a medical device removal in violation of the Federal Food, Drug, and Cosmetic Act (FDCA).

June 6, 2019 Fort Washington Man Sentenced to 66 Months in Federal Prison for Two Separate Drug Cases. U.S. District Judge Paul W. Grimm sentenced Daniel Mark Wilkerson, age 45, of Fort Washington, Maryland today to 66 months in federal prison, followed by five years of supervised release, for possession with intent to distribute more than 100 kilograms of marijuana, and in a separate case for conspiring to steal prescription drugs from federal military hospitals. Judge Grimm also ordered that Wilkerson pay restitution of $4,450,679.60, and forfeit $16,320.44.

June 5, 2019 Opioid Manufacturer Insys Therapeutics Agrees to Enter $225 Million Global Resolution of Criminal and Civil Investigations. As part of the civil resolution, lnsys agreed to pay $195 million to settle allegations that it violated the False Claims Act. As part of the criminal resolution, lnsys will enter into a deferred prosecution agreement with the government, lnsys's operating subsidiary will plead guilty to five counts of mail fraud, and the company will pay a $2 million fine and $28 million in forfeiture.

June 3, 2019 Government Contractor Pleads Guilty To Making False Statements. Enco Industries, Inc., a company located in Plaistow, New Hampshire, pleaded guilty to making false statements to the U.S. Department of Defense's Defense Logistics Agency, announced United States Attorney Scott W. Murray.

June 3, 2019 United States Files False Claims Act Complaint Against South Carolina Chiropractor, Pain Management Clinics, Urine Drug Testing Laboratories, and Substance Abuse Counseling Center. The United States has filed a complaint under the False Claims Act against Daniel McCollum, a chiropractor based in Greenville, South Carolina, and pain management clinics and urine drug testing laboratories that McCollum owned or managed for engaging in illegal financial relationships and providing medically unnecessary services and items, including urine drug testing and steroid injections and prescriptions for opioids and lidocaine ointment, the Department of Justice announced today.

Fraud Detection Resources for Auditors from DoD OIG

The Inspector General Act of 1978, Section 8(c)(3), requires the Inspector General of the Department of Defense to "provide policy direction for audits and investigations relating to fraud, waste, and abuse."

The following links to resources can help increase an auditor's awareness of possible audit risk factors, as well as their responsibilities for audit planning, executing, reporting, and referring the matter to the appropriate investigative organization when an audit identifies fraud indicators.

The resources highlight key generally accepted government auditing standards (GAGAS), requirements, and overall DoD audit expectations and best practices for identifying and detecting

potential fraud. GAGAS describes fraud as: a type of illegal act involving the obtaining of something of value through willful misrepresentation. Whether an act is, in fact, fraud is a determination to be made through the judicial or other adjudicative system and is beyond the auditor's professional responsibility. However, the various scenarios and the accompanying fraud indicators describe situations related to some common fraud schemes that DoD auditors might encounter.

Our resources include:

- General Fraud Scenarios and Indicators,
- Fraud Red Flags and Indicators, and
- Contract Audit Fraud Detection Resources.

DoD employees must disclose any known fraud, abuse, corruption, mismanagement, or waste to the appropriate DoD, Federal government, other appropriate official, or hotline. DoD employees are also encouraged to report any suspected irregularities indicating that fraud, waste, abuse, corruption, or mismanagement may have occurred or may be ongoing. Individuals should be able to make all disclosures without the fear of reprisal.

DoD auditors or non-Federal government auditors performing audits for the DoD have additional responsibilities. The DoD OIG expects auditors to be proactive in identifying and referring to the appropriate investigative organization known or potential fraud, abuse, or corruption. By maintaining a high level of fraud awareness and appropriately assessing fraud risk during the planning and execution phases, the auditor is better positioned to uncover fraudulent acts. DoD auditors must adhere to their fiduciary responsibilities to the DoD, the Federal government, and the public.

Auditor Responsibilities

Auditors who perform independent audits and attestation engagements of DoD organizations, programs, activities, and functions are required by DoD Instruction (DoDI) 7600.02, "Audit Policies," to comply with the GAGAS issued by the Comptroller General of the United States. The GAGAS require auditors when performing financial and performance audits and examination-level attestation engagements (work that requires a positive assurance) to:

- identify risk factors (indicators),
- assess the risk associated with those factors (indicators),
- design and perform appropriate steps and procedures to address the risk areas,
- document the process, and
- include information on any potential fraud that might have a material impact on the audited subject matter in the report.

Auditors should design procedures to obtain reasonable assurance of detecting fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, and abuse that could materially affect the audit or examination. For review-level (work that provides negative assurance) and agreed-upon procedures-level (provides no opinion or assurance) attestation engagements, auditors are not required to assess fraud risk factors or design steps to address those risks.

Auditors must perform procedures when they find information or indicators that fraud may have occurred that could materially impact the subject matter under review. In those cases, auditors should determine whether the fraud was likely to have occurred and, if so, determine the effect on the results of the engagement. GAGAS requires auditors to comply with any legal requirements to report known or likely fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse directly to parties outside the audited entity.

DoDI 7600.02, paragraph 6.3, establishes the requirement that auditors shall refer to the appropriate investigative organization any indications of potential fraud or other criminal acts discovered while performing audit work.

Best Practices

Best practices for DoD audit organizations include identifying and assessing potential fraud risks factors during the planning phase for review-level and agreed-upon procedures attestation engagements similar to what the auditor does for other audit services or work. When risk factors are identified during the planning phase, the auditor should discuss with their supervisor or higher-level management whether the requested or planned review-level or agreed-upon-procedures-level engagement is appropriate.

With audit management approval, auditors should discuss with the requestor the fraud risk factors and whether an alternative type of audit or attestation engagement would be more appropriate. When the auditor identifies fraud indicators or other information that strongly points to a high probability of fraud during the planning phase, the auditor, after consulting with their management, should raise their concerns to the appropriate oversight or investigative organization.

Best practices also include designing some steps or procedures to address identified risk factors for a review-level attestation engagement. While DoD auditors are required to comply with GAGAS, other auditing standards may provide insight into best practices or other approaches to assessing fraud risks or identifying fraud indicators. The GAGAS incorporates the American Institute of Certified Public Accountants (AICPA) standards for fieldwork and reporting for financial audits and attestation engagements.

The AICPA auditing standards for financial audits and the GAGAS for financial and performance audits provide specific steps that are not included in the AICPA or the GAGAS for attestation engagements such as inquiring of management about potential fraud. Auditors may find these specific steps useful when considering how to best implement GAGAS for attestation engagements. Similarly, audit organizations may learn about other audit organizations' approaches and methods for assessing fraud risks and identifying and detecting fraud indicators and adapt best practices when feasible.

U.S. Department of Agriculture OIG

The Office of Inspector General of the U.S, Department o Agriculture (USDA) was legislatively established in 1978 with the enactment of the Inspector General Act (Public Law 95-452). The act requires the Inspector General to independently and objectively:

- Perform audits and investigations of the Department's programs and operations;
- Work with the Department's management team in activities that promote economy, efficiency, and effectiveness or that prevent and detect fraud and abuse in programs and operations, both within USDA and in non-Federal entities that receive USDA assistance;
- Report OIG activities to the Secretary and the U.S. Congress semiannually as of March 31 and September 30 each year;

This is accomplished by:

- investigating allegations of fraud and abuse;
- auditing the economy and efficiency of USDA programs and operations, including program results, the security of information technology, compliance with applicable laws and regulations, and the accuracy of financial reports;
- applying predictive analytics, statistical modeling, computer matching, and data mining and warehousing to USDA programs and operations.

USDA OIG is headquartered in Washington, D.C., and has regional offices located in Atlanta, Georgia; Beltsville, Maryland; Kansas City, Missouri; Chicago, Illinois; New York, New York; Oakland, California; and Temple, Texas.

USDA OIG emphasizes service to management at all levels of the Department by briefing senior Department officials on major audits and investigations. They also work proactively with agency managers, as part of a united team, by directly encouraging management input into the audit and investigative process to help solve difficult problems impacting program management and operations. As a member of the Council of the Inspectors General on Integrity and Efficiency (CIGIE), they also participate with other Inspectors General in multi-agency projects where the issues are crosscutting and need to be addressed Government-wide. The strategic goals of the USDA OIG are:

- Strengthen USDA’s ability to implement and improve safety and security measures to protect the public health, as well as agricultural and Departmental resources.
- Reduce program vulnerabilities and strengthen program integrity in the delivery of program assistance.
- Provide USDA with oversight to help it achieve results oriented performance.

USDA, much like other agencies and departments throughout the Government, faces challenges in overseeing its many programs. USDA employs nearly 100,000 employees in 17 agencies and 18 staff offices; in total, these employees operate approximately 300 programs responsible for delivering about $143 billion in public services annually. Overseeing these programs so every dollar spent accomplishes the intended results poses significant challenges to USDA program managers.

USDA has made some progress improving accountability for its programs when the Office of Inspector General (OIG) or other third parties, such as GAO, have identified deficiencies. For example, after OIG received a complaint concerning recent changes in how the Natural Resources Conservation Service (NRCS) makes determinations regarding whether a wetland exists on a given tract of land, OIG reviewed determinations made in the "prairie pothole region" (Iowa, Minnesota, North Dakota, and South Dakota). It was found that, to address a backlog of requests for wetland determinations, NRCS made significant changes in its process for wetland determinations that allowed producers to drain and farm more wetlands. However, the agency did not execute the process for making this change in a transparent manner. NRCS generally agreed with the finding and recommendations to issue official guidance reinforcing correct and current rules and clarifying procedures for making wetland determinations and certifications, including the status of pre-1996 determinations.

Similarly, USDA's Office of Homeland Security and Emergency Coordination (OHSEC) has taken steps to improve oversight and management controls over handling of classified material. In 2013, OIG made 17 recommendations about the Department's internal management controls over classified material. In a subsequent audit, it was found that OHSEC management did not supply adequate oversight to monitor audit follow-up activities performed by its staff, as OIG found that 11 recommendations were not addressed at the time of our fieldwork. Weaknesses existed in four other recommendations. Such weaknesses introduced a higher potential for misclassification, over-classification, and unauthorized release of national security information within USDA. OHSEC has stated that it completed implementation of previous recommendations and revised guidance and processes to improve management oversight, as was recommend in the most recent report.

OIG audits consistently show that USDA agencies need to strengthen oversight and accountability over their programs. For example, OIG recently reviewed OHSEC's actions related to agroterrorism preparedness. Agroterrorism is a threat to national security and could result in increased human illnesses and deaths, widespread destruction of crops and livestock, and significant economic loss to the Nation's farmers and ranchers. OIG found that OHSEC had not adequately overseen and coordinated USDA's efforts to prevent, detect, and respond to agroterrorism. Also, OHSEC did not demonstrate that USDA was in compliance with Homeland Security Presidential Directive 9 requirements to defend the agriculture and food system against terrorist attacks, major disasters, and other emergencies.

The OIG has found that despite actions to improve information technology (IT) security, USDA continues to display weaknesses in planning, management, and oversight of its cybersecurity initiatives that affect the Department's compliance with standards for safeguarding IT systems as directed in the Federal Information Security Modernization Act of 2014 (FISMA). The degree to which USDA complies with FISMA and other security guidance directly correlates to the security posture of each agency and office. USDA senior management needs to make sure agencies and offices understand how implementation of IT security directly impacts USDA's overall security posture. For USDA to attain a security posture that is secure and sustainable, all 35 of its agencies and offices must consistently implement Departmental policy based on a standard methodology. When every agency and office is in compliance with USDA's policies,

USDA as a whole will be compliant with FISMA and, more importantly, have a sustainable security posture.

Due to prior outstanding recommendations and weaknesses related to IT and FISMA, OIG will continue to report a material weakness in USDA's IT security that should be included in the Department's annual Federal Managers Financial Integrity Act report. OIG concluded that the Department lacks an effective information security program.14 OCIO has not implemented corrective actions that the Department committed to in response to prior OIG recommendations. In a report released in 2016, OIG found that from FYs 2009 through 2015 they had made 61 recommendations for improving the overall security of USDA's systems. OCIO implemented corrective action for 39 of those recommendations, but testing identified that security weaknesses still exist in 3 of those closed recommendations. OCIO should revisit these three areas. Also, a number of recommendations have exceeded the specified corrective action implementation dates. If the planned corrective actions to close out these recommendations are no longer achievable due to budget cuts or other reasons, then OCIO needs to update those corrective action plans and request a change in management decision in accordance with Departmental guidance.

In that report, OIG also found that policies and programs designed to address FISMA requirements have not been completed or fully implemented, and USDA has not fully developed an organizational perspective that includes a comprehensive governance structure and organization-wide risk management strategy. Governance is a set of processes that ensures the effective and efficient use of IT in enabling an organization to achieve its goals. A nonexistent governance structure will continue to leave USDA's IT security program in a reactive state, continuously struggling to adapt to changing conditions. In order to resolve these far-reaching IT security problems, senior USDA management needs to develop a governance structure that will encourage compliance at both the agency and Departmental level. This should improve the Department's overall security posture and FISMA score.

Designing, developing, and implementing programs that reliably achieve their intended results has been a recurring challenge for the Department. OIG has found that agencies do not have adequate reviews or controls in place to supply the metrics necessary to evaluate program performance. In some programs, the strategy for measuring performance is missing altogether. As a result, some agencies are using inaccurate or unreliable data in program performance reports.

Currently, USDA manages approximately 300 programs that provide a variety of services and financial assistance to the American public. This diverse portfolio of programs means that, for the Department to serve as a diligent steward of Federal funds, USDA must have well-designed programs with clear goals and performance measures.

The Government Performance and Results Modernization Act of 2010 set requirements for regular and recurring program performance assessment. In keeping with the law, an agency should have controls in place that allow it to regularly review a program's performance, and then compile reports that allow it to measure that performance. These reports allow the Department to evaluate fairly its programs' successes and failures.

Due to ongoing efforts to establish and develop outcome-based performance measures, the Department has made progress in measuring the actual success of its programs. In FY 2015, OIG found that USDA's programs for supporting beginning farmers, funded by different agencies, could benefit from a thorough revision of how they report program results. Since FY 2015, USDA has developed an integrated, coordinated strategy to ensure that these programs help new farmers establish and sustain new farming operations. As part of this strategy, the Department provides direction to agencies for defining consistent and measurable outcomes, clearly articulates desired outcomes, develops milestone dates for goals, and creates a timeline to ensure agencies accomplished all mandated duties from the 2008 Farm Bill. This direction has helped agencies improve their coordination and more consistently define eligibility requirements for their programs for beginning farmers and ranchers.

USDA has emphasized its efforts to improve outreach to new and beginning farmers and ranchers, local and regional food producers, minorities, women, and veterans. As part of those efforts, the Department has stressed the importance of civil rights, highlighting that significant progress needs to be made in working with communities when addressing past civil rights issues. Due to a history of public attention concerning how USDA has treated members of socially disadvantaged groups, the Department faces challenges in earning those groups' trust.

In recent years, OIG has completed audits intended to help resolve long-standing complaints against USDA. The Food, Conservation, and Energy Act of 2008 directed that all pending claims and class actions (for example, Pigford v. Glickman, Garcia v. Vilsack, and Love v. Vilsack) brought against USDA by socially disadvantaged farmers or ranchers, including Hispanics and women, based on racial, ethnic, or gender discrimination in farm program participation, be resolved in an expeditious and just manner. OIG reviews of the claims administration process for these class actions generally found that the process for resolving these complaints was strong, and appropriate payments were being made to eligible farmers.

OIG also performed audits designed to help the Department improve outreach to socially disadvantaged groups. For example, OIG evaluated the effectiveness of the Department's activities related to providing assistance to beginning farmers and ranchers. USDA agencies have provided significant financial resources and technical support to beginning farmers to assist in the establishment and sustainability of farming operations. It was found, however, that the Department had not developed an integrated and coordinated strategy to ensure effective implementation. The Department also lacked sufficient performance goals, direction, coordination, and monitoring to ensure success. Since USDA spent $3.9 billion in beginning farmers' assistance in FYs 2012 and 2013, it is critical that the Department ensure that these funds are benefiting those intended.

There are several recommendations outstanding related to a review we performed of FSA's Microloan Program. The Microloan Program is intended to create new economic opportunities through farming. The Microloan Program offers flexible access to credit and serves as an attractive loan alternative for smaller farm operations, including nontraditional farm operations, which often face limited financing options. However, it was found that FSA could not demonstrate that it successfully reached out to some targeted audiences, such as specific

underserved groups and veterans. The low percentage of participation by some targeted groups suggests FSA needs to increase its outreach to those underserved groups.

OIG concluded that the Food Safety and Inspection Service (FSIS) has taken action to improve food safety and the humane handling of animals at the plants FSIS inspects. However, it was found that FSIS continues to face challenges gathering reliable data to ensure safety verification tasks are completed, effective, and consistent. FSIS also continues to face challenges in training, documenting and tracking, overseeing, testing, and verifying that the Nation's commercial supply of meat, poultry, and egg products complies with regulatory requirements.

Although FNS has endeavored to improve management controls for the Supplemental Nutrition Assistance Program (SNAP), weaknesses continue to exist in controls over administrative tasks, benefit distribution, and quality control (QC) processes. The potential exists for billions of dollars of taxpayer-funded assistance not to be delivered or used as intended.

As the largest benefit program within USDA and one of the largest in the Federal Government, SNAP presents a unique challenge for the program's managers. In FY 2016, SNAP provided monthly food assistance for nearly 44 million low-income individuals and disbursed almost $67 billion in benefits. Given SNAP's size and significance, fraud, waste, and abuse are critical concerns. OIG's audit work focuses on improving the efficiency of program administration and maintaining the integrity of Federal funds. Further, USDA loses hundreds of millions of dollars every year to fraud and crime associated with SNAP and other FNS food assistance programs. OIG devotes significant investigative resources to recover that money and prosecute criminals. In the first half of FY 2017, OIG's investigative efforts related to SNAP resulted in 171 indictments, 187 convictions, and 511 arrests, with a total dollar impact of $54.9 million.

In FY 2016, FNS made a number of improvements to SNAP management controls. In FY 2016, OIG found that FNS' oversight of State agency controls over able-bodied adults without dependents (ABAWD) could be improved. FNS improved administrative oversight of ABAWD provisions by updating the Management Evaluation Management System (MEMS) to MEMS Next Generation in 2016. MEMS allowed FNS to track reports to States, including management evaluations and financial management reviews, and provided a central repository of schedules for all reviews and reports. However, it did not always contain complete information on ABAWD management evaluations due to confusion regarding data entry procedures. Prior to implementing MEMS Next Generation, FNS provided necessary training and training manuals to ensure employees used the system correctly. These improvements demonstrate FNS' commitment to ensuring the effective and efficient delivery of services to eligible SNAP recipients.

U.S. Department of Commerce OIG

The Inspector General provides overall leadership and policy direction for OIG, and reviews proposed and existing departmental legislation and regulations. The IG keeps the Secretary, Deputy Secretary, and Congress informed of serious problems and deficiencies relating to the administration of the Department's programs and operations, recommends corrective actions, and reports on the progress made in implementing corrective actions. The Office of Counsel provides legal advice and assistance to the IG and to OIG staff engaged in the other principal activities. The Office of Administration provides OIG-wide support in the areas of budget and administration, human resources, and information technology.

The mission of the Department of Commerce (DOC) OIG is to improve the programs and operations of the DOC through independent and objective oversight. The vision of the OIG is stated as:

- To be recognized for our contribution to improved Commerce performance.
- We work as a seamless, integrated team delivering valuable products to serve the public and to support decision-makers in the Department, OMB, and Congress.
- We are an integral and trusted broker to our stakeholders.
- We are catalysts for positive change throughout the Department.
- We are fully staffed and have the resources to get the job done.
- We have a diverse, competent, enthusiastic, and productive workforce and a cadre of effective managers at every level of the organization.
- We have credible risk assessment processes that drive strategic and operational plans, priorities, and programs.
- We have efficient, effective processes and a state-of-the-art infrastructure.
- We have performance metrics that drive high performance and accountability.

Core values of the office are Integrity, Excellence, and Accountability.

Integrity

- We are honest, ethical, and objective.
- We hold ourselves to high standards and are willing to take tough stands.
- We honor our commitments to each other and our stakeholders.

Excellence

- We are forward-looking and seize opportunities to improve Commerce performance
- We deliver timely, relevant, and high-impact products and services.
- We encourage risk-taking that leads to new ideas and innovative solutions.

Accountability

- We operate as independent, transparent, and trusted brokers serving our stakeholders.
- We are passionate about delivering results that drive positive change.
- We are trustworthy and can be counted on to do what we say.

Oversight Areas of the OIG are:

Office of the Secretary

Bureau of Economic Analysis
Bureau of Industry and Security
U.S. Census Bureau
Economic Development Administration
Economics and Statistics Administration
International Trade Administration
Minority Business Development Agency
National Oceanic and Atmospheric Administration
National Telecommunications and Information Administration
National Institute of Standards and Technology
National Technical Information Service
U.S. Patent and Trademark Office

Audits and Evaluations

The Office of Audit and Evaluation (OAE) provides executive leadership and management for the consolidated audit and evaluation activities conducted by the Office of Inspector General in monitoring Commerce operations, as well as external activities funded by the Department through contracts or financial assistance (loans, grants, and cooperative agreements).

OAE audit and evaluation activities include performance audits and evaluations, and financial audits. OAE also reviews and handles resolution of certain single audits conducted by state and local auditors on recipients of Commerce financial awards. All audit work is performed in accordance with government auditing standards.

Performance audits and evaluations address the efficiency, effectiveness, and economy of the Department's programs, activities, and information technology systems. They may check a unit's compliance with laws and regulations, and evaluate its success in achieving program objectives. They may also assess the operations of a contractor or recipient of a Commerce financial assistance award to determine whether the recipient complied with laws, regulations, and award terms; claimed allowable project costs; and achieved intended results.

Financial audits determine whether a reporting entity (1) has presented its financial statements fairly and in accordance with generally accepted accounting principles; (2) has an internal control structure that provides reasonable assurance of achieving the control objectives set forth by OMB; and (3) has complied with laws and regulations that could have a direct and material effect on its financial statements, the Federal Financial Management Improvement Act, and other laws and regulations.

Single audits. The Single Audit Act establishes audit requirements for state and local government and nonprofit organizations receiving federal financial assistance. In addition to undergoing OIG-performed audits, certain recipients of Commerce financial assistance undergo single audits conducted by state and local government auditors and independent public accountants. OAE reviews all single audit reports that have findings, and works with the funding agency and the recipients to resolve them.

OAE's audits and evaluations may be prompted by congressional requests from committees and individual Members, or by statute. We perform annual audits of Commerce financial statements pursuant to the Chief Financial Officers Act of 1990 and information security reviews as required by the Federal Information Security Management Act of 2002.
Investigations

The Office of Investigations (OI) investigates alleged or suspected fraud, waste, abuse, and misconduct by Commerce employees, contractors, recipients of financial assistance, and others involved in the Department's programs and operations. Such wrongdoing may result in criminal and/or civil prosecution, as well as administrative sanctions for violations of Department regulations and employee standards of conduct. OI's significant areas of criminal work are as follows:

- Contract and grant fraud. OI investigates fraudulent activity related to grant awards made by Commerce operating units as well as contracts entered into by the Department and its operating units.

- Employee misconduct. OI investigates or assists the Department in handling employee misconduct involving Commerce funds and programs. These cases cover a wide range of improper behavior—from misusing one's official position to stealing government property—that may warrant administrative sanction or criminal prosecution.

- Support for other law enforcement offices. OI often partners with other law enforcement agencies to investigate cases involving Commerce employees as victims or perpetrators of crimes not directly related the business of the Department.

Below is a summary of the OIG final report, issued November 14, 2018, on the Department’s top management and performance challenges for FY 2019.

Challenge 1: Successfully Completing 2020 Census Testing and Systems Integration of New Innovations in Time to Deliver a Cost-Effective, Accurate Decennial Census. Our FY 2019 top management and performance challenges include these priority areas related to the 2020 Census:

- Minimizing the challenges associated with incomplete testing of 2020 Census systems and innovations
- Mitigating the risks of unplanned changes
- Preventing further reductions to cost avoidance, reducing cost overruns, and eliminating unaccounted-for costs

Challenge 2: Maximizing Efficiencies of Environmental Satellite Programs. Our FY 2019 top management and performance challenges include these priority areas related to NOAA’s satellite programs:

- Reducing life-cycle costs of the Polar Weather Satellite (PWS) program
- Identifying an optimal launch strategy for remaining satellites in the series
- Managing risks in next-in-series satellites
- Planning an optimal next-generation satellite system architecture

Challenge 3: Deploying a Nationwide Public Safety Broadband Network (NPSBN). Our FY 2019 top management and performance challenges include these priority areas related to the First Responder Network Authority (FirstNet):

- Deploying the NPSBN
- Securing public safety participation
- Ensuring the successful performance of the contract awarded to AT&T
- Ensuring effective and efficient use of proceeds AT&T provides annually to FirstNet
- Strengthening operational controls

Challenge 4: Ensuring USPTO Provides High-Quality Intellectual Property Rights. Our FY 2019 top management and performance challenges include these priority areas related to USPTO:

- Ensuring that the Patent Trial and Appeal Board operates fairly and effectively.
- Ensuring that examiners perform thorough patent application reviews
- Improving the management of information technology (IT) acquisitions and operations

Challenge 5: Continuing to Improve the Department's Cybersecurity Posture. Our FY 2019 top management and performance challenges include these priority areas related to the Department's cybersecurity posture:

- Implementing security controls to protect the systems supporting the 2020 Census
- Securing cloud-based systems and assets• Sustaining Department-wide implementation of the Continuous Diagnostics and Mitigation program
- Maintaining a robust IT workforce to manage an effective IT security program

Challenge 6: Utilizing Resources and Developing Processes to Rebalance Trade Enforcement and Promotion Priorities. Our FY 2019 top management and performance challenges include these priority areas related to trade enforcement and promotion:

- Building staff expertise for the self-initiation of antidumping and countervailing duty cases
- Institutionalizing processes for Section 232 product exclusion request reviews and managing the increased foreign investment review workload
- Managing the downsizing of trade promotion capacity

Challenge 7: Providing Adequate Oversight to Effectively Manage the Significant Increase in Disaster Assistance Funding to EDA. Our FY 2019 top management and performance challenges include these priority areas related to EDA disaster relief:

- Following a comprehensive oversight implementation strategy
- Acquiring and maintaining sufficient staff with appropriate proficiency
- Developing a risk management strategy to strengthen internal control

Challenge 8: Addressing Departmental Management Matters Involving Acquisitions. Our FY 2019 top management and performance challenges include these priority areas related to acquisitions:

- Improving monitoring of blanket purchase agreements (BPAs)

- Developing and maintaining a competent acquisition workforce to support the Department's mission
- Establishing oversight of mission-support service delivery
- Increasing the pace of NOAA ship acquisitions

Many of the audits and evaluations performed in the last few years have been in preparation for the 2020 census. The following are examples of the type of findings by the OIG:

06.19.2019 The Census Bureau Must Correct Fundamental Cloud Security Deficiencies in Order to Better Safeguard the 2020 Decennial Census

02.06.2019 2020 Census: Issues Observed During the 2018 End-to-End Census Test's Address Canvassing Operation Indicate Risk to Address List Quality

10.30.2018 The Census Bureau Must Improve Its Implementation of the Risk Management Framework

07.30.2018 Census Bureau Could Improve Monitoring of Blanket Purchase Agreements by Complying with Key Federal Acquisition Regulation and Commerce

04.30.2018 2020 Census: The Number and Location of Area Census Offices May Not Reflect NRFU Workload Demands and Will Not Result in Projected Cost Savings

02.27.2018 2020 Census: The Bureau's Background Check Office Is Not Fully Prepared for the 2020 Census

09.25.2017 Awarding of U.S. Census Bureau Noncompetitive Contracts Did Not Consistently Follow Federal Acquisition Regulations and Commerce Acquisition Policies

09.13.2017 2020 Census: Evaluation of Interactive Review Address Canvassing Operation Revealed Issues with Quality Assurance Controls

05.11.2017 2020 Census: The Address Canvassing Test Revealed Cost and Schedule Risks and May Not Inform Future Planning as Intended

03.29.2017 2020 Census: Census Bureau Needs to Improve Controls over Administrative Records

03.16.2017 2020 Census: 2016 Census Test Indicates the Current Life-Cycle Cost Estimate is Incomplete and Underestimates Nonresponse Followup

06.07.2016 2020 Census: The Bureau Has Not Reported Test Results and Executed an Inadequately Designed 2015 Test

04.18.2016 The Census Working Capital Fund Lacks Transparency

02.23.2016 Census Bureau Reviews of Unliquidated Obligations Could Be Improved with Greater Review Frequency and Additional Documentation

02.23.2016 The U.S. Census Bureau's Efforts to Ensure an Accurate Address List Raise Concerns over Design and Lack of Cost-Benefit Analysis

U.S. Department of Transportation OIG

The Office of Inspector General (OIG) is committed to fulfilling its statutory responsibilities and supporting members of Congress, the Secretary, senior Department officials, and the public in achieving a safe, efficient, and effective transportation system. Since OIG was established in 1979, we have been dedicated to providing independent and objective reviews of the economy, efficiency, and effectiveness of Department of Transportation (DOT) programs and operations, and to detecting and preventing fraud, waste, abuse, and criminal violations of laws affecting DOT.

By law, the Inspector General (IG) reports to the Secretary of Transportation and Congress. OIG is the principal law enforcement office within DOT with authority to carry firearms, execute warrants, and make arrests. OIG often collaborate with other Federal, State, and local law enforcement entities, and must report possible criminal violations to the U.S. Attorney General. OIG's Office of Investigations also manages our Hotline Complaint Center that is staffed 24 hours a day, 7 days a week. This office is also responsible for investigating whistleblower complaints, including those referred by the U.S. Office of Special Counsel.

OIG's Office of Auditing and Evaluation is comprised of auditors, analysts, information technology experts, economists, statisticians, engineers, accountants, and other subject matter experts. In addition to performance audits aimed at improving the economy, efficiency, and effectiveness of transportation programs, our audit staff specialize in financial management, information technology, and acquisition and procurement audits. While OIG's work is akin to that of private sector auditors and management consultants, OIG reports are made available to the public via the USDOT website.

OIG neither issues regulations nor sets departmental policy. OIG's role is to provide facts for the policy-makers in the Department and Congress. One of OIG's key deliverables is our statutorily required annual report on DOT's top management challenges (TMC), which provides a forward looking assessment for the coming fiscal year to aid DOT's operating administrations in focusing attention on the most serious management and performance issues facing the Department. For fiscal year 2019, OIG identified eight major challenges facing DOT:

1. Effectively implementing FAA's new safety oversight strategy
2. Protecting against a wide range of threats to aviation safety and security
3. Maintaining focus on the railroad industry's implementation of positive train control
4. Improving NHTSA's data use, processes, and oversight of vehicle safety defects
5. Providing effective stewardship over surface infrastructure safety and investments
6. Modernizing the National Airspace System while introducing new capabilities and making sound investment decisions
7. Systematizing cybersecurity strategies to deter surging cyber threats
8. Harnessing innovative procurement and financing practices while maintaining oversight of acquisitions, grants, and assets

OIG investigates allegations of fraud, waste, abuse, and other violations of law by DOT employees, contractors, grantees, and regulated entities. Some of the most significant issues we investigated fiscal year 2019 include:

- Highway safety. A Virginia trucking company was ordered to pay $3.25 million in forfeiture, fines, and restitution for violating FMCSA safety regulations designed to prevent fatigue related crashes.
- Hazardous waste materials safety. As a result of OIG investigation, a Michigan man was convicted for a scheme to distribute human body parts infected with diseases (such as HIV and hepatitis) to customers requesting cadavers for medical and dental training.
- Employee integrity. OIG special agents brought a former FAA employee to justice for making thousands of dollars in unauthorized personal purchases and cash withdrawals using Government credit cards.
- Grant and procurement fraud. A New York R&D firm agreed to forfeit nearly $5 million in assets after our investigation uncovered its multimillion-dollar research grant fraud scheme.
- Aviation safety. As a result of OIG investigation, a South Florida man was sentenced to 7 years in prison for multiple fraud schemes against FAA, including flying a commercial carrier without an airman's certificate.
- Amtrak. A former Amtrak contracting officer plead guilty to a $7.6-million bribery scheme in which he steered contracts and provided pricing information to a company for about $20,000 in bribes and other valuable items, including trips to the beach.
- Disadvantaged Business Enterprise (DBE) fraud. OIG special agents brought a Pennsylvania bridge painting contractor and project manager to justice for their involvement in a $4.5-million DBE fraud scheme.

OIG conducts independent and objective audits and reviews of DOT programs and activities to ensure they operate economically, efficiently, and effectively. Some of the significant issues reviewed fiscal year 2019 include:

- Detention and delays. OIG estimates that average truck crash rates increase 6.2% with every 15 minutes a truck is delayed at a shipping and receiving facility. Detention may also reduce driver and carrier income over $1 billion annually.
- NextGen. FAA manages $1.7 billion in NextGen developmental projects using project level agreements. However, 12 of the 22 agreements OIG sampled did not align with FAA's high-priority areas.
- Cybersecurity. In all five function areas (Identify, Protect, Detect, Respond, and Recover), OIG found DOT's information security program and practices to be at the Defined maturity level—the second lowest tier of the information security maturity model.
- Referral of criminal activity. OIG made recommendations to help DOT and its Operating Administrations help enable prompt referrals of fraud, waste, abuse, or other criminal violations to DOT OIG.
- FAA's office and warehouse leases. FAA's office and warehouse leases represent a potential value of $1.4 billion. OIG estimates that FAA could have put $37.6 million to

better use by addressing various weaknesses in its management of leased offices and warehouses.

- FAA's maintenance technicians. As directed by the House Committee on Appropriations, OIG assessed FAA's plans for hiring and placing its approximately 6,000 maintenance technicians who play a vital role in repairing, replacing, and certifying air traffic equipment.
- Light passenger vehicle recalls. OIG audit found that NHTSA's management of light passenger vehicle recalls lacks adequate processes for monitoring recalls and verifying recall completion rates.

Appendix A: History of Federal Offices of Inspector General

Read the Inspector General Act of 1978, as amended. 

2016
In December, the Inspector General Empowerment Act was enacted to exempt OIGs from requirements of the Paperwork Reduction Act and Computer Matching Act, and guaranteed full and timely IG access to all agency records and materials related to DOT programs and operations, except where the IG's right of access is otherwise expressly limited by statute. The Act also added changed several new reporting requirements for IGs and altered the structure and timeframes under which the Integrity Committee of the Council of the Inspectors General on Integrity and Efficiency operates.

2009
In February, the American Recovery and Reinvestment Act was enacted to create and save American jobs and spur economy activity. That Act also created the Recovery Accountability and Transparency Board, on which the DOT IG serves as a member, to provide transparency and prevent and detect fraud, waste and abuse in relation to Recovery Act funds.

2008
On October 14, the IG Reform Act consolidated the PCIE and ECIE into the Council of the Inspectors General on Integrity and Efficiency (CIGIE) as the unified council of all statutory Federal IGs to provide government-wide coordination of, and focus on, the activities of the OIGs. The IG Reform Act also amended provisions of the IG Act of 1978 related to the appointment and removal of IGs, IG pay, providing independent counsel for IGs, submission of OIG budget requests, and OIGs operating as discrete and separate agencies, among other things.

2005
OIGs joined together to play a key part in oversight of activities and expenditures directly linked to recovery from the devastating Gulf Coast hurricanes (Katrina and Rita).

2004
The temporary Iraq governing body, the Coalition Provisional Authority, was abolished and its IG converted to the Special IG for Iraq Reconstruction. This concept of creating Special IGs for specific purposes and limited terms is subsequently used again to address emerging risks in 2008, resulting in the creation of the Special IG for Troubled Asset Relief Program and the Special Inspector General for Afghanistan Reconstruction.

2003
The IG community updated The Silver Book—Quality Standards for Federal Offices of Inspector General. In March, the Transportation Security Administration and the U.S. Coast Guard, and related OIG responsibilities, were transferred from the Department of Transportation to the new Department of Homeland Security created by the Homeland Security Act of 2002. On December 1, President George W. Bush signed S.J. Res 18, a joint Congressional Resolution, commending IGs for their efforts to prevent and detect waste, fraud, abuse, and mismanagement

and to promote economy, efficiency, and effectiveness in the federal government during the past 25 years.

2002
To enhance the federal government's information technology security, Congress passed the Federal Information Security Management Act (FISMA), which requires IGs to conduct an annual evaluation of the information security programs and practices of their respective agencies. Also in 2002, the Homeland Security Act, signed by President George W. Bush, granted law enforcement powers to certain OIG criminal investigators. That Act amended the IG Act of 1978 to authorize special agents at most presidentially appointed OIGs to exercise law enforcement authority, including carrying firearms, making arrests, and executing warrants, and included provisions to enable other OIGs to qualify for law enforcement authority as well. Prior legislation had given this authority to only four OIGs.

2001
In the aftermath of the September 11 terrorist attacks, the IGs came together to contribute to efforts to address the protection of the Nation’s physical and information technology infrastructure.

1996
Executive Order 12993, signed by President William J. Clinton on March 21, established procedures for a special Integrity Committee to independently investigate allegations of wrongdoing by individual IGs.

1995
The IG community issued the first Journal of Public Inquiry, a semiannual publication providing a forum to share professional ideas, suggest new approaches, and chronicle changes over the years.

1992
Executive Order 12805, signed by President George H.W. Bush on May 11, established the Executive Council on Integrity and Efficiency (ECIE), for the DFE OIG community and reconstituted the PCIE.

1990
In order to improve the federal government's financial management, Congress passed the Chief Financial Officers Act, which directed IGs to audit the annual financial statements produced by federal agencies.

1988
The IG Act was amended to create 30 additional OIGs at Designated Federal Entities (DFE). Most of the DFEs are relatively small agencies, boards, or commissions. These IGs have essentially the same powers and duties as those appointed by the President; however, the DFE IGs are appointed by, and can be removed by, the head of their affiliated agency.

1981
Executive Order 12301, signed by President Ronald Reagan on March 26, established the President's Council on Integrity and Efficiency (PCIE) comprised of presidentially appointed IGs.

1979
On February 25, 1979, Secretary Brock Adams signed a Determination Order formally establishing the Office of Inspector General within the U.S. Department of Transportation. Following a transfer of certain DOT audit and investigative personnel and functions to the OIG, Secretary Adams further clarified in a memorandum dated April 27, 1979, that other than investigation programs involving odometer fraud and U.S. Coast Guard officer and elisted personnel, there should be no auditor or criminal investigator personnel employed in DOT other than within the Office of Inspector General.

1978
On October 12, 1978, the Inspector General (IG) Act established twelve Federal Offices of Inspector General (OIG), including the Department of Transportation OIG. The Act passed the House of Representatives by a vote of 388 to 6 and was later approved by the Senate by unanimous consent. Two OIGs had previously been established, one in 1976 and another the following year. President Jimmy Carter signed the IG Act into law and described the new statutory IGs as “perhaps the most important new tools in the fight against fraud.” The President charged the IGs to always remember that their ultimate responsibility is not to any individual but to the public interest.