Office of the Inspector General:

Review of Seven Offices

Compiled and Edited by

Michael Erbschloe

Connect with Michael on LinkedIn

©2019 Michael Erbschloe

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.

Thank You for previewing this eBook

You can read the full version of this eBook in different formats:

- HTML (Free /Available to everyone)
- PDF / TXT (Available to V.I.P. members. Free Standard members can access up to 5 PDF/TXT eBooks per month each month)
- Epub & Mobipocket (Exclusive to V.I.P. members)

To download this full book, simply select the format you desire below

Free-Ebooks.net