



OFFICE OF THE SECRETARY

Top Management and Performance Challenges Facing the Department of Commerce

FINAL REPORT NO. OIG-16-049

SEPTEMBER 30, 2016

U.S. Department of Commerce
Office of Inspector General
Office of Audit and Evaluation


FOR PUBLIC RELEASE





September 30, 2016

INFORMATION MEMORANDUM FOR THE SECRETARY

FROM: David Smith 
Deputy Inspector General

SUBJECT: *Top Management and Performance Challenges Facing the Department of Commerce in Fiscal Year 2017*

Enclosed is our final report on the Department of Commerce's top management and performance challenges for fiscal year (FY) 2017. We have aligned our report with the Department's FYs 2014–2018 Strategic Plan—and, within each of the plan's strategic goals, we discuss the challenges we have identified.

1. TRADE AND INVESTMENT: Expand the U.S. economy through increased exports and foreign direct investment that leads to more and better American jobs.

Departmental and bureau grants oversight. The Department and its bureaus with grant programs must consolidate the various Departmental grants management systems into one system. An additional challenge is identifying, hiring, and maintaining a qualified financial assistance workforce.

2. INNOVATION: Foster a more innovative U.S. economy—one that is better at inventing, improving, and commercializing products and technologies that lead to higher productivity and competitiveness.

- *USPTO patent examinations.* Despite the increase in both the number of patent examiners and spending on patent examination, USPTO still faces challenges in meeting its targets for patent processing time. In addition, USPTO continues to face challenges in enhancing patent quality and developing more effective quality metrics.
- *USPTO information technology (IT) systems.* For FY 2017, USPTO requested \$595.6 million from Congress for its IT portfolio. As stated in its 2014–2018 Strategic Plan, USPTO's vision for the next 4 years includes plans to continue transforming its operations with next-

generation technology and services. However, USPTO still needs to deploy a significant number of applications within the portfolios and, in the interim, must rely on more than 67 existing legacy systems to conduct day-to-day business.

- *FirstNet network implementation.* As FirstNet makes progress in acquisition activities, consultation, and internal control, challenges remain. FirstNet plans to award a contract for the development and management of a nationwide public safety broadband network (NPSBN) in November 2016. Also, NTIA issued \$116.56 million in grant awards under the Middle Class Tax Relief and Job Creation Act of 2012's State and Local Implementation Grant Program to promote—among each of the 56 states and territories, as well as tribes and federal public safety entities—outreach, data collection, and planning for the NPSBN. In addition, various government and accounting reports have identified the need for FirstNet to strengthen its controls.
- *Demand for radio frequency spectrum.* Freeing up spectrum for high-speed broadband services remains a key challenge facing the Department. In June 2010, the President directed the Department, working through NTIA, to make 500 megahertz of federal and non-federal spectrum available by 2020 to support wireless broadband needs. As of June 2016, NTIA reported that it has made available almost half of the 500 megahertz goal. NTIA continues to investigate opportunities to make additional spectrum available, while ensuring no loss of critical existing and planned federal, state, local, and tribal government capabilities.

3. ENVIRONMENT: Ensure communities and businesses have the necessary information, products, and services to prepare for and prosper in a changing environment.

- *NOAA satellite acquisitions.* The Department must manage risks associated with the acquisition and development of environmental satellite systems. Satellite integration and test problems caused NOAA to delay the Geostationary Operational Environmental Satellite-R Series (GOES-R) estimated launch date to November 2016. If the launch date continues to be delayed, there will be increased risk of a potential gap in coverage. Also, in order for the Joint Polar Satellite System (JPSS) program to launch JPSS-1 by the end of the second quarter of FY 2017, it must investigate and correct a problem with a key instrument, as well as complete environmental and other final tests of the satellite and a major upgrade of the JPSS common ground system.

- *NOAA observational data processing.* The ground system development problems that both GOES-R and JPSS-1 are addressing may necessitate the deferral of planned operational capabilities until after their launches. Management attention to post-launch test activities is needed to ensure users' needs are met—and inform a new Administration and Congress of data availability and its effect on forecasts.
- *NOAA National Marine Fisheries Service data.* NOAA Fisheries must balance two competing interests: promoting commercial and recreational fishing while preserving populations of fish and other marine life. Developing conservation and management measures requires collecting, analyzing, and reporting demographic information about fish populations via stock assessments. NOAA continues to face challenges to ensuring timely and accurate stock assessments and providing what is often controversial consultation to its stakeholders.

4. DATA: Improve government, business, and community decisions and knowledge by transforming Department data capabilities and supporting a data-enabled economy.

- *2020 Census quality and cost.* On October 1, 2015—after conducting FYs 2013, 2014, and 2015 site tests—the Bureau released its 2020 Census Operational Plan, with a set of design decisions that drive how the 2020 Census will be conducted. The Bureau plans to conduct additional testing in order to refine the design. Its 2017 site test must be adequately planned and implemented to ensure critical information is obtained. In addition, audits continue to report deficiencies in the Bureau's cost accounting practices, which will make it difficult for the bureau to demonstrate that cost savings were realized. Without complete cost information, it will be difficult for the Bureau to compute accurate estimates and actual costs for comparison with budget requests.
- *Census enterprise data system.* The Census Enterprise Data Collection and Processing System (CEDCaP) Program aims to integrate and standardize the Bureau's systems in order to share data collection and processing across all censuses and surveys. Specifically, CEDCaP proposes to consolidate costs by retiring unique, survey-specific systems and redundant capabilities—a factor in the proposed redesign with a goal of realizing an estimated \$5 billion in costs avoidance for the 2020 decennial census. A challenge the Program faces is how to effectively integrate, test, and implement the architecture and systems to a level sufficient enough to support the 2017 Census site test, the 2018 end-to-

end decennial test, and the 2020 Census itself, all within a short timeframe.

- *Departmental compliance with the Digital Accountability and Transparency Act of 2014 (DATA Act).* The DATA Act requires federal agencies to make available detailed information on their spending and use of federal funds and reporting it by specific categories, such as how much funding an agency receives from Congress and how much agencies spend on specific projects and awards. Due to the Department's legacy information systems and need to use existing funding resources, providing reliable and consistent agency program information and meeting the goals of the DATA Act will be a significant challenge.
- *Replacement for Commerce Business Systems (CBS).* The lack of a centralized and integrated financial management system continues to create reporting and oversight challenges for the Department—including the ability to effectively report financial data and monitor financial activity across its operating units. The Department and most of its operating units' continued reliance on CBS—with its limited functionality, high support costs, lack of system integration, and lack of centralized reporting capabilities—is an immediate high risk for the Department's compliance with current and future reporting requirements such as the DATA Act.

5. OPERATIONAL EXCELLENCE: Strengthen the Department's capacity to achieve its objectives, maximize return on program investments, and deliver quality, timely service.

- *Department-wide IT security issues.* We continue to find deficiencies in the implementation of basic security measures, such as regularly identifying vulnerabilities, expeditiously remediating security flaws, and effectively managing access controls. As a result of these deficiencies, Department systems continued to face the significant risk of cyber attacks. Also, continuing the implementation of the enterprise security operations center and enterprise cybersecurity monitoring and operations is critical to providing timely cyber situational awareness across the Department. Accordingly, the Department needs to make the required management commitment and prioritize resources to fully implement these cybersecurity initiatives.
- *The Department's contracts and acquisitions.* A government-wide initiative notes that excessive reliance on sole-source and cost-

reimbursement contracts creates risk of waste, inefficiency, and misuse. Our work across the Department continues to identify that—without sound procurement practices and an effective acquisition structure in place—the risk of wasted government dollars increases. During FY 2015, the Department made significant gains in managing and strengthening the acquisition workforce but still faces related challenges.

- *IT controls for financial data.* The independent auditor of the Department’s annual financial statements reported general IT controls as a Department-wide significant deficiency in FYs 2012–2015. Specifically, the Department’s financial systems continue to have deficiencies in the areas of access controls, configuration management, and segregation of duties within their financial management system. In addition, a significant deficiency related to IT access and configuration management control weaknesses was identified in the USPTO’s annual financial statement audit in FY 2015. The Department and USPTO have ongoing efforts in place to implement corrective actions for the deficiencies identified.
- *Department-wide culture of accountability.* One major challenge is detecting and preventing time and attendance abuse, which OIG has investigated at several Departmental operating units. Another challenge involves the integrity of procurement processes: over the past 3 fiscal years, OIG conducted multiple investigations into allegations of abuse in contracting matters. In addition, in FY 2016, OIG investigated alleged abuses related to official Department travel. These inquiries raised concerns about the Department’s compliance with governing laws and rules, particularly the Federal Travel Regulation and the Department’s travel-related policies.

We remain committed to keeping the Department’s decision-makers informed of problems identified through our audits and investigations so that timely corrective actions can be taken. The final version of the report and the Department’s response to it (which appears as an appendix) will be included in the Department’s *Annual Financial Report*, as required by law.¹

¹ 31 U.S.C. § 3516(d).

We appreciate the cooperation received from the Department, and we look forward to working with you and the Secretarial Officers in the coming months. If you have any questions concerning this report, please contact me at (202) 482-4661.

cc: Bruce Andrews, Deputy Secretary of Commerce
Kelly R. Welsh, General Counsel
Joshua G. Berman, Deputy General Counsel
Steve Cooper, Chief Information Officer
Ellen Herbst, Chief Financial Officer and Assistant Secretary
for Administration
Jim Hock, Chief of Staff to the Secretary
Operating Unit Heads
Operating Unit Audit Liaisons

Contents

Departmental Strategic Goal 1: TRADE AND INVESTMENT	1
Managing systems and personnel related to the processing of grants	1
Departmental Strategic Goal 2: INNOVATION	2
Improving process time and quality of patent application examinations	2
Transitioning from legacy IT systems to next-generation IT systems	3
Addressing the challenges of ensuring the successful procurement and monitoring of a nationwide high-speed, broadband network dedicated to public safety	3
Addressing the increasing demand for radio frequency spectrum	5
Departmental Strategic Goal 3: ENVIRONMENT	6
Managing environmental satellite system acquisition and development risks	6
Establishing life-cycle cost and schedule baselines for Polar Follow-On program	8
Preparing to process observational data from GOES-R series and JPSS-1	8
Balancing the priorities of sustainable fisheries with those of multiple stakeholders	9
Departmental Strategic Goal 4: DATA	10
Delivering a timely 2020 Census that maintains or improves data quality but costs less than the 2010 Census	10
Delivering CEDCaP in time to support the 2020 Census workload volume	12
Achieving the mandate for government-wide data standards of the DATA Act	12
Identifying a long-term solution to replace CBS	13
Departmental Strategic Goal 5: OPERATIONAL EXCELLENCE	14
Continuing to implement basic information security measures and expeditiously remediate critical and high-risk vulnerabilities	14
Implementing the Department’s cybersecurity improvement initiatives	15
Managing high-risk and noncompetitive contracts	16
Managing and strengthening the acquisition workforce	17
Improving IT controls for financial data processed on the Department’s systems	17
Creating a Department-wide culture of accountability	18
Appendix A: Related OIG Publications	19
Appendix B: List of Acronyms	22

Departmental Strategic Goal I: TRADE AND INVESTMENT

Expand the U.S. economy through increased exports and foreign direct investment that leads to more and better American jobs

The Department faces a challenge to comply with new requirements from the Office of Management and Budget (OMB) regarding grant administration, which became effective in December 2014. The new approach places a greater burden on the Department and, if not properly implemented, may affect the performance of its trade and research grant programs. Our fiscal year (FY) 2017 *Top Management and Performance Challenges* report focuses on managing systems and personnel related to the processing of grants.

Managing systems and personnel related to the processing of grants

The Department continues to face challenges in its effort to consolidate the various Departmental grants management systems into one system. A single grant system is expected to reduce costs overall by consolidating interfaces and feeder systems and result in more efficient and effective administrative and business management. The Economic Development Administration (EDA) and the National Institute of Standards and Technology (NIST) continue to work with the National Oceanic and Atmospheric Administration (NOAA) to consolidate their grant management systems to the NOAA Grants Online (GOL) system. The system migration for the grant program on EDA's system began in 2014, with an estimated completion for October 2017. At this time, most EDA programs have migrated to GOL. However, the latest completion estimates are December 2017 for final migration of the EDA system and April 2018 for the NIST system. NOAA will be challenged to obtain funding, issue contracts for the work, and complete migration on time.

Another challenge is identifying, hiring, and maintaining a qualified financial assistance workforce. Unlike acquisitions personnel, those who monitor grants and cooperative agreements are not required to obtain or maintain their professional education through a formal, standardized certification program. Budget constraints and the lack of a required certification program for those in the Grants Management Specialist occupational series challenge bureaus' ability to identify and attract experienced financial assistance professionals.

Departmental Strategic Goal 2: INNOVATION

Foster a more innovative U.S. economy—one that is better at inventing, improving, and commercializing products and technologies that lead to higher productivity and competitiveness

To foster a more innovative U.S. economy and strengthen U.S. manufacturing, the Department has many diverse innovation programs. These include programs within the U.S. Patent and Trademark Office (USPTO), the First Responder Network Authority (FirstNet), and the National Telecommunications and Information Administration (NTIA). Our FY 2017 *Top Management and Performance Challenges* report focuses on the following:

- USPTO improving process time and quality of patent application examinations;
- USPTO transitioning to next-generation information technology (IT) systems;
- NTIA and FirstNet successfully procuring and monitoring a nationwide public safety broadband network (NPSBN), effectively consulting with stakeholders, and addressing internal control, staffing, and other issues; and
- NTIA addressing the increasing demand for radio frequency spectrum through sharing among federal and commercial entities.

Improving process time and quality of patent application examinations

Between FY 2011 and FY 2015, the number of USPTO patent examiners increased by 34 percent, from 6,685 to 8,977. Over the same period, actual budget obligations for patent examination increased by 39 percent, from \$1.37 billion to \$1.91 billion. Despite the increase in the number of patent examiners and the increase in spending on patent examination, USPTO still faces challenges in meeting its targets for patent processing time. Specifically, in FY 2015, average first action pendency was 17.3 months while its target pendency was 16.4 months. For average total pendency, USPTO has made improvements in reducing the pendency to 26.6 months, meeting its target pendency of 27.7 months. However, USPTO still faces challenges for meeting its long-term goal of 10 months for the average first action pendency, and 20 months for the average total pendency by FY 2019.

The USPTO also faces a long-standing challenge to ensure that it issues high-quality patents to help protect patent applicants from litigation arising from ambiguous or overly broad patents—as well as reduce abusive patent litigation by so-called “patent trolls.” For FYs 2011–2015, USPTO adopted the composite quality metric to track performance of various factors that affect quality and to provide a single comprehensive metric representing the overall state of patent examination quality. However, in April 2015, we reported that USPTO’s official quality metrics may underrepresent the true rate of errors associated with patent quality.¹ Further, through the Enhanced Patent Quality Initiative (EPQI) launched in FY 2015, USPTO received feedback that the composite quality metric did not adequately reflect quality.

¹ Department of Commerce Office of Inspector General, April 10, 2015. *USPTO Needs to Strengthen Patent Quality Assurance Practices*, OIG-15-026-A. Washington, DC: DOC OIG, 10.

In response, USPTO terminated the use of the composite quality metric at the end of FY 2015 and, working with its stakeholders, increased its focus on ensuring that it issues correct and clear patents. The new patent quality metric will focus on the correctness and clarity of the patent examiner's actions. According to USPTO, through correctness and clarity, such patents better enable potential users of patented technologies to make informed decisions on how to avoid infringement, whether to seek a license, and/or when to settle or litigate a patent dispute. The USPTO also states that patent owners will also benefit from having clear notice on the boundaries of their patent rights.

It is too early for OIG to assess whether the EPQI will improve patent quality. As a result, USPTO continues to face challenges for enhancing patent quality and developing more effective patent quality metrics that encompass statutory compliance and clarity of decision making by patent examiners.

Transitioning from legacy IT systems to next-generation IT systems

USPTO relies on technology services to examine applications, manage rights, and collect revenues associated with patents and trademarks. For FY 2017, the agency requested \$595.6 million from Congress for its IT portfolio.

As stated in its 2014–2018 Strategic Plan, USPTO's vision for the next 4 years includes plans to continue transforming its operations with next-generation technology and services. USPTO currently relies on over 67 legacy systems that support nearly every aspect of its business operations. USPTO has begun the development and deployment of some of its major IT portfolio systems—such as Patent End-to-End, Trademark Next Generation, and Patent Trial and Appeal Board End-to-End—and has begun phasing out legacy systems as they are replaced.

However, USPTO still needs to deploy a significant amount of applications within the portfolios and, in the interim, must rely on the existing legacy systems to conduct day-to-day business. USPTO will therefore continue to be challenged to deploy in a timely manner all projects within the portfolios. The agency must ensure that these end-to-end systems achieve full capabilities, while balancing the need to maintain legacy systems until they are replaced. In addition, USPTO has various business units with unique operational considerations and challenges—and must continue collaborating with these business units to ensure the delivery of tools to meet their business needs.

Addressing the challenges of ensuring the successful procurement and monitoring of a nationwide high-speed, broadband network dedicated to public safety

The Middle Class Tax Relief and Job Creation Act of 2012 (the Act) established FirstNet as an independent authority to implement a nationwide broadband network dedicated for first responders.² While outlining the next phase of FirstNet's Strategic Roadmap in March 2016, FirstNet Chair Sue Swenson stated “we have laid out an aggressive schedule to ensure progress continues along the Roadmap in coordination with public safety, the states, and Federal

² Pub. L. No. 112-96; see also 47 U.S.C. § 1426.

agencies.”³ As FirstNet makes progress in acquisition activities, consultation, and internal control, the following challenges remain:

Effective management of acquisitions. In January 2016, FirstNet issued a request for proposals (RFP) for the development, build, and management of an NPSBN. Proposals were due May 31, 2016, and FirstNet—with assistance from the Department of Interior’s Acquisitions Services Directorate—must effectively evaluate proposals to select the best vendor solution.

FirstNet adopted an objectives-based approach in its RFP—rather than a traditional requirements-driven model—to provide industry the maximum opportunity and flexibility in the development of innovative solutions for the NPSBN. The successful bid must meet the objective-based goals of the RFP. Also, as the RFP points out, FirstNet must provide services at competitive prices, given constrained local, state, and federal budgets. Further, FirstNet must be self-sustaining—by leveraging existing infrastructure, obtaining optimal value for excess network capacity, and optimizing its pricing structure.

FirstNet plans to award the contract in November 2016. Once the contract is awarded, FirstNet will need to provide adequate and appropriate contract oversight, which may require resource adjustment within the organization.

Effective consultation with states and localities. FirstNet is required by the Act to consult with the 56 states and territories, as well as tribes and federal public safety entities in order to build and deploy an effective NPSBN.⁴ NTIA issued \$116.56 million in grant awards under the Act’s State and Local Implementation Grant Program (SLIGP) to promote associated outreach, data collection, and planning for the NPSBN. FirstNet must continue to work with designated points-of-contact at each location and entity to assess public safety needs and develop individual state plans for building and deploying radio access networks that result in a nationwide design that meets public safety needs.

Continue to strengthen internal control. Reports issued by OIG,⁵ the Government Accountability Office,⁶ and an independent public accounting firm⁷ have identified the need for FirstNet to strengthen its controls. Our recent audit of FirstNet’s management of its interagency agreements (IAAs) found that FirstNet could strengthen controls regarding documenting IAA tracking and closeout procedures; we also noted that FirstNet could maintain readily available

³ First Responder Network Authority. March 16, 2016. *FirstNet Continues Momentum Toward Network Deployment With New Strategic Roadmap Milestones, Spectrum Relocation Grant Program* [online].

See <http://www.firstnet.gov/news/firstnet-continues-momentum-toward-network-deployment-new-strategic-roadmap-milestones-spectrum> (accessed August 10, 2016).

⁴ 47 U.S.C. § 1426(b)(1).

⁵ See DOC OIG, December 5, 2014. *FirstNet Must Strengthen Management of Financial Disclosures and Monitoring of Contracts*, OIG-15-013-A. Washington, DC: OIG. See also DOC OIG, August 14, 2015. *Audit of FirstNet’s Workforce and Recruiting Challenges, Participation at Discretionary Outreach Events, and Internal Control*, OIG-15-036-A. Washington, DC: OIG.

⁶ U.S. Government Accountability Office, April 2015. *FirstNet Should Strengthen Internal Controls and Evaluate Lessons Learned*, GAO-15-407. Washington, DC: GAO.

⁷ Harper, Rains, Knight & Company, July 22, 2015. *Independent Auditors’ Report*.

documentation and provide timely responses to audit requests to demonstrate transparency and accountability of programs and operations.⁸

Addressing the increasing demand for radio frequency spectrum

Freeing up radio frequency spectrum to meet the increasing demand for high-speed broadband services—while ensuring no loss of critical existing and planned federal, state, local, and tribal government capabilities—remains a key challenge facing the Department. In June 2010, the President directed the Department, working through NTIA, to make 500 megahertz of federal and non-federal spectrum available by 2020 to support wireless broadband needs.⁹ In June 2013, federal agencies were further directed to expand the availability of spectrum by accelerating efforts to share federal spectrum with non-federal users.¹⁰

As of June 2016—6 years after the President’s 2010 directive, and with 4 years remaining to achieve the goal—NTIA reported that it has made 245 megahertz of spectrum available, which is almost half of the 500 megahertz goal. NTIA continues to investigate opportunities to make additional spectrum available by conducting studies, consulting with the Federal Communications Commission, and undertaking research and development (R&D) activities to better understand spectrum-sharing capabilities between federal and non-federal users. Additionally, NTIA continues to search for a replacement system for the Federal Spectrum Management System (FSMS), which was terminated in 2015. FSMS was intended to support federal spectrum management by (1) identifying and managing spectrum for federal use and (2) identifying and releasing spectrum for non-federal use.

As the 2020 target approaches, NTIA’s challenge is to incorporate lessons learned from its R&D activities and consultation efforts into actual strategies that lead to more efficient use and availability of radio frequency spectrum. Also, the termination of FSMS necessitates that the Department identify a technological system that can modernize, automate, and integrate key spectrum management functions.

⁸ DOC OIG, June 29, 2016. *FirstNet Can Strengthen Its Controls by Documenting Procedures to Close and Track Interagency Agreements*, OIG-16-035-A. Washington, DC: OIG.

⁹ The White House Office of the Press Secretary, June 28, 2010. “Unleashing the Wireless Broadband Revolution,” Memorandum for the Heads of Executive Departments and Agencies [online]. <https://www.whitehouse.gov/the-press-office/presidential-memorandum-unleashing-wireless-broadband-revolution> (accessed August 17, 2016).

¹⁰ The White House Office of the Press Secretary, June 14, 2013. “Expanding America’s Leadership in Wireless Innovation,” Memorandum for the Heads of Executive Departments and Agencies [online]. <https://www.whitehouse.gov/the-press-office/2013/06/14/presidential-memorandum-expanding-americas-leadership-wireless-innovatio> (accessed August 17, 2016).

Departmental Strategic Goal 3: ENVIRONMENT

Ensure communities and businesses have the necessary information, products, and services to prepare for and prosper in a changing environment

The Department must actively manage risks associated with the acquisition and development of the next generation of NOAA environmental satellites. These satellites provide data and imagery used to track severe storms, forecast weather, and study climate and other environmental conditions. While NOAA works to improve forecast prediction, severe weather preparedness, and its stewardship over marine resources, habitats, and ecosystems, our FY 2017 *Top Management and Performance Challenges* report focuses on the following:

- launching the first satellite in the Geostationary Operational Environmental Satellite-R Series (GOES-R) program in the first quarter of FY 2017 and testing the second satellite (GOES-S) in parallel;
- completing spacecraft and ground system testing of Joint Polar Satellite System-I (JPSS-I) in the first quarter of FY 2017 and launching in the second quarter of FY 2017, under the next-generation JPSS program;
- finalizing life-cycle costs, baselines, and launch strategies for the Polar Follow-on program (JPSS-3 and JPSS-4);
- preparing to process observational data from these next-generation polar and geostationary satellite systems; and
- balancing the priorities of sustainable fisheries with those of multiple stakeholders.

Managing environmental satellite system acquisition and development risks

The Department must manage risks associated with the acquisition and development of environmental satellite systems. NOAA's major satellite system programs are among the Department's largest investments, totaling more than 16 percent of its \$9.7 billion FY 2017 budget request.¹¹

NOAA geostationary and polar-orbiting environmental satellites provide some of the most important data and imagery for weather forecasting and storm tracking. NOAA's GOES-R and JPSS programs have their first and second launches, respectively, scheduled for the first and second quarters of FY 2017. Both are facing similar challenges completing the integration and testing of satellites and ground systems. At the same time, the programs are developing or planning for additional satellites.

Our work on these programs has highlighted the need for effective management to mitigate the potential for gaps in the environmental data provided by NOAA's current, aging systems.

Completing and launching GOES-R series satellites. A number of satellite integration and test problems caused NOAA to delay the GOES-R estimated launch date from March 2016 to

¹¹ Total of FY 2017 budgets for GOES-R, JPSS-I, and Polar Follow-On programs from the "NOAA FY 2017 Budget Submission."

November 2016. Most recently, a launch anomaly on an international space station resupply mission in March raised concerns about GOES-R's launch vehicle. After an investigation and corrective actions, GOES-R's launch date was postponed from October to November 2016. If the launch date continues to slip, there will be increased risk to NOAA's ability to maintain a spare, on-orbit satellite, as well as a potential gap in coverage.

Threats to the GOES-R launch schedule include problems with its ground system. In April 2016, independent testing identified concerns with two antennas that could corrupt satellite communications and cause a loss of operational data and products. The program's risk assessment noted the possibility that additional antennas may degrade in a similar manner, resulting in an insufficient number of antennas to support launch, on-orbit commissioning, post-launch testing, and operations.

GOES-R development issues and schedule delays have affected the progress of the program's next mission, GOES-S. In February 2016, NOAA slipped the GOES-S launch commitment date from May 2017 to the fourth quarter of FY 2018. The GOES-R mission's problems pulled resources away from the GOES-S effort, and in some cases required the use of GOES-S components as spares for GOES-R.

Completing preparations for the launch of JPSS-I. The JPSS program is committed to launching JPSS-I no later than the end of the second quarter of FY 2017. Before then it must complete environmental and other final tests of the satellite and a major upgrade of the JPSS common ground system.

The program had to significantly revise the integration and testing sequence of activities for JPSS-I in order to accommodate the delayed completion of the Advanced Technology Microwave Sounder (ATMS) and pivoted support systems (gimbals) for the satellite's two science mission data antennas. We reported in April 2016 that JPSS-I's schedule reserves¹² were below the program's procedural requirements. The satellite's environmental testing campaign began in mid-March. In July 2016, testing detected additional problems with ATMS that required its removal from the satellite in order to investigate and correct. The program chose to delay its planned launch date from January 20, 2017, to no earlier than March 16, 2017, leaving little margin to its launch commitment date.¹³

The JPSS-I launch is also contingent upon an upgrade of the JPSS common ground system. This major upgrade will provide new hardware and software, capabilities for supporting JPSS-I, a full backup capability, additional ground antenna stations, multiple operating environments, and significant security improvements. Its completion has been prolonged by software development and integration problems, adding risk to the JPSS-I launch schedule.

In April 2016—before the discovery of additional problems with ATMS—we concluded that the program's ability to meet full requirements for JPSS-I launch was at risk. Further, the program's

¹² This referred to schedule reserves toward what was then a January 20, 2017, planned launch date.

¹³ Dates are as of August 2016, according to JPSS program management reports.

need to revise its integration and testing approach to preserve its schedule risked having lower-level system requirements insufficiently tested.¹⁴

Recently, the importance of launching JPSS-1 has taken on added urgency. The JPSS program has been responding to more frequent issues with Suomi National Polar-orbiting Partnership (Suomi NPP), which was launched in 2011 and will reach the end of its designed mission life in November 2016. Suomi NPP is the only provider of certain JPSS-quality information from the afternoon polar orbit. The loss of that data before JPSS-1 is in operation would result in a data gap that could affect the accuracy of weather forecasts. Although JPSS-1 is committed to launch by the end of March 2017, data is not expected to be available until June 2017 at the earliest.

Establishing life-cycle cost and schedule baselines for Polar Follow-On program

The JPSS program has been formulating the acquisition and development of two additional satellites—JPSS-3 and JPSS-4—which will be copies of JPSS-2. Funded in FY 2016 under the Polar Follow-On program budget, the missions will be integrated with and managed by the JPSS program. In April 2016, we reported that the program had to postpone formulation milestones intended to support the establishment of cost and schedule baselines.

The program's conception of a robust architecture for polar satellites stems from a NOAA independent review team recommendation that (1) two failures must occur to create a gap in microwave or infrared sounding data and (2) the ability exists to restore the constellation to a two-failure condition within 1 year. To meet the second criterion, the program was planning to build JPSS-3 and JPSS-4, and store the satellites until needed or by their scheduled launch dates. However, NOAA's polar satellite launch policy did not include such a strategy; we recommended that NOAA incorporate the robust architecture criteria into formal policy.¹⁵ The launch strategy for JPSS-3 and JPSS-4 will need to be well-defined in order to understand its cost and schedule implications.

Preparing to process observational data from GOES-R series and JPSS-1

The ground system development problems both programs are addressing may necessitate the deferral of planned operational capabilities until after the launches of GOES-R and JPSS-1. Management attention to post-launch test activities is needed to ensure users' needs are met—and to inform a new Administration and Congress of data availability and its effect on forecasts.

In our April 2016 report, we noted that the National Weather Service was planning to make operational use of JPSS-1 data in early 2018—approximately 1 year after its launch—but would be completing a contingency plan to expedite the use of the data, if needed. Given the potential for a data gap as Suomi NPP approaches the end of its design life, we made recommendations that the weather service complete the contingency plan and communicate it to users and stakeholders by the end of the third quarter of FY 2016. We also recommended that NOAA

¹⁴ DOC OIG, April 26, 2016. *The Joint Polar Satellite System: Further Planning and Executive Decisions Are Needed to Establish a Long-term, Robust Program*, OIG-16-026-I. Washington, DC: OIG, 12–13.

¹⁵ *Ibid.*, 19.

provide stakeholders with a list of key activities for operationalizing JPSS-I data that NOAA will undertake during the potential gap period.

Balancing the priorities of sustainable fisheries with those of multiple stakeholders

The National Marine Fisheries Service (NOAA Fisheries) must balance two competing interests: (1) promoting commercial and recreational fishing as vital elements of our national economy and (2) preserving populations of fish and other marine life. The Magnuson-Stevens Act of 1976, the Marine Mammal Protection Act of 1972, and the Endangered Species Act of 1973 (Endangered Species Act) gave NOAA Fisheries responsibility for rebuilding and maintaining sustainable fisheries and promoting the recovery of protected marine species. The Magnuson-Stevens Act also made NOAA Fisheries the primary federal agency for managing marine fisheries and established a regional fishery management council system to help the agency carry out its mission.

Developing conservation and management measures requires collecting, analyzing, and reporting demographic information about fish populations via stock assessments. These assessments are a key element of the fishery management process; they are used to determine whether additional regulations are necessary to rebuild fish stocks or whether an increase in fishing opportunities can be allowed. Because of their potential impact on commercial and recreational fishing, these assessments are often controversial, and the methods used to create the estimates typically undergo intense scrutiny by the fishing industry, conservation groups, and other stakeholders who at times question the assessments and subsequent fishery management decisions, such as total allowable catch determinations.

Under the authority of section 7 of the Endangered Species Act, NOAA also provides consultations to other federal agencies on those entities' activities that may affect a threatened or endangered species. These interagency consultations are designed to assist federal agencies in fulfilling their duty to ensure federal actions do not jeopardize the continued existence of a species or destroy or adversely modify critical habitat. Many of the agency's opinions have been the subject of legal challenges and political controversy.

NOAA continues to face challenges to ensuring timely and accurate stock assessments and providing what is often controversial consultation to its stakeholders.

Departmental Strategic Goal 4: DATA

Improve government, business, and community decisions and knowledge by transforming Department data capabilities and supporting a data-enabled economy

The Department produces large amounts of data that are vital in the 21st century information-driven economy, benefitting businesses, governments, and the public. A major data source of the Department, the Census Bureau, faces challenges as it prepares for the 2020 decennial census. Also, the Digital Accountability and Transparency Act of 2014 (DATA Act) compels federal departments and agencies to expand data capabilities and support a data-enabled economy. Our FY 2017 *Top Management and Performance Challenges* report focuses on the following:

- the Census Bureau planning a 2020 Census that maintains the data quality of the 2010 Census, while improving cost efficiency;
- the Census Bureau delivering the Census Enterprise Data Collection and Processing System (CEDCaP) in time to support the 2020 Census workload volume;
- achieving the mandate for government-wide data standards of the DATA Act; and
- identifying a long-term solution to replace Commerce Business Solutions (CBS).

Delivering a timely 2020 Census that maintains or improves data quality but costs less than the 2010 Census

During the decade leading up to (and during) the 2010 Census, the Census Bureau's decennial program experienced several major changes. For example, its plans to automate field data collection had to be greatly curtailed. Problems developing and implementing handheld computers and related automation compelled the Bureau to abandon its plans to use the devices during the nonresponse followup (NRFU) operation and forced it to make late-stage preparations for a pen-and-paper NRFU. The Bureau also rejected using the Internet and administrative records (which were intended to contain costs and improve accuracy) and made a substantial investment to conduct a full, nationwide address canvassing operation to update its address list just prior to the decennial enumeration.

After conducting FYs 2013, 2014, and 2015 site tests—which focused on using technology and design innovations—the Bureau released its 2020 Census Operational Plan on October 1, 2015. The plan is comprised of a set of design decisions that drive how the 2020 census will be conducted. Design innovations aimed at reducing the costs of fieldwork focus on four key areas: (1) reengineering address canvassing, (2) optimizing self-response, (3) utilizing administrative records and third-party data, and (4) reengineering field operations. The most expensive activities associated with the 2020 Census are expected to be the address canvassing and NRFU operations field costs.

Although some design decisions—such as rejecting the use of administrative records and abandoning an automated NRFU operation—were based on evidence obtained during site tests, the Bureau plans to conduct additional testing in order to refine the design. The need for additional testing, coupled with the May 2016 decision to use a commercial off-the-shelf

(COTS) platform—rather than continue to use internally built systems which were tested during the 2015 and 2016 site tests—means the Bureau’s 2017 site test must be adequately planned and implemented to ensure critical information is obtained. However, past audits¹⁶ have identified deficiencies in the Bureau’s planning process, such as not developing measurable success criteria; not designing test activities to answer research questions; and not analyzing and documenting test results in time to incorporate changes into subsequent tests, which may impact the effectiveness of the 2017 site test. With less than a year left until the start of the 2017 site test, the Bureau must resolve planning deficiencies while ensuring this critical test is designed to provide anticipated results.

Implementing a new address canvassing approach. For the 2010 census, the address canvassing operation mobilized thousands of field workers to canvass almost every street in the United States and Puerto Rico to update the Census Bureau’s address list and map data. To reduce address canvassing costs for the 2020 Census, the Bureau has implemented a new process that intends to identify stable geographic areas that do not require updating. The new process includes (1) a block-by-block in-office imagery review, (2), a second office review using local government or third party information (referred to as active-block resolution) where change has been identified, and (3) for blocks that cannot be resolved through an office review, in-field address canvassing. The Bureau estimates this new approach will save an estimated \$900 million. However, this cost avoidance is based on reducing in-field address canvassing to approximately 25 percent of the total number of addresses in the areas that could receive a mailed questionnaire. While in-office address canvassing during the first quarter of the fiscal year appears to indicate the 25 percent goal is being achieved, the new address canvassing process is in the beginning stages and has not been validated. If the in-field canvassing goal of 25 percent cannot be achieved, the costs for conducting the new process are higher than estimated, or the results of the new process are unsatisfactory and require additional work, then anticipated cost reductions may not be realized.

Effectively recording, collecting, and using financial data to ensure cost savings are achieved. The Census Director stated in November 2015¹⁷ that a redesigned 2020 Census is estimated to cost \$12.5 billion compared to a cost of \$17.8 billion that it would take to repeat the paper and pencil design of the 2010 Census. The \$5.2 billion in cost avoidance is calculated based on implementing changes in the four key innovation areas. However, audits continue to report deficiencies in the Bureau’s cost accounting practices which will make it difficult for the bureau to demonstrate that cost savings were realized. Specifically, the Bureau must capture costs during field tests to inform estimates and develop a method for allocating contractor costs to 2020 decennial projects in order to report the full project cost. Without complete cost

¹⁶ See DOC OIG, September 30, 2015. *2020 Census: The 2014 Census Test Misses an Opportunity to Validate Cost Estimates and Establish Benchmarks for Progress*, OIG-15-044-A. Washington, DC: OIG. See also DOC OIG, June 7, 2016. *2020 Census: The Bureau Has Not Reported Test Results and Executed an Inadequately Designed 2015 Test*, OIG-16-032-A. Washington, DC: OIG.

¹⁷ Census Bureau, November 3, 2015. *Written Testimony of John H. Thompson, Director of the U.S. Census Bureau, Before the U.S. House of Representatives Subcommittee on Government Operations and the Subcommittee on Information Technology of the Committee on Government Oversight and Reform*. Washington, DC: Census Bureau. See http://www.census.gov/content/dam/Census/about/about-the-bureau/20151103_thompson_testimony.pdf.

information, it will be difficult for the Bureau to provide stakeholders with accurate estimates and actual costs that can be compared to budget requests.

Delivering CEDCaP in time to support the 2020 Census workload volume

The CEDCaP Program is an initiative to create an integrated and standardized system of systems that will offer shared data collection and processing across all censuses and surveys. Specifically, the program proposes to consolidate costs by retiring unique, survey-specific systems and redundant capabilities. The Bureau estimates that CEDCaP costs will be lower than the cost of 2010 decennial systems. Also, CEDCaP is integral to the Bureau's plan of achieving its estimated \$5.2 billion costs avoidance goal for the 2020 decennial census.

The CEDCaP Program is comprised of 12 projects that will deliver enterprise solutions which will provide core capabilities and enabling technologies for enterprise data collection and processing. The Bureau announced in May 2016—after conducting a COTS Capability Assessment and Analysis—that it will implement a hybrid solution for CEDCaP. The CEDCaP hybrid solution will deliver six of the planned capabilities through a vendor solution and the remaining six through systems developed in-house. Given this decision, the CEDCaP program office has several time-sensitive acquisition and technical decisions to make to ensure adequate staffing, integration, and implementation of the vendor platform and in-house solutions. Therefore, a challenge the Program faces is how to effectively integrate, test, and implement the architecture and systems—which include a cloud-based solution for internet self-response—to a level sufficient enough to support the 2017 Census site test; the 2018 end-to-end decennial test; and, ultimately, the 2020 Census, all within a short timeframe. It is conceivable that—with the current funding, staffing challenges, and unexpected project delays—some systems might be tested for the first time during the final end-to-end test.

Achieving the mandate for government-wide data standards of the DATA Act

The DATA Act requires federal agencies to make available to the public detailed information on their spending and use of federal funds. Further, the DATA Act requires reporting by specific categories, such as how much funding an agency receives from Congress and how much agencies spend on specific projects and awards, as well as the use of common government-wide data standards when posting this financial information for public use—standards that are not currently applied across all agencies for all uses. In addition, agencies must ensure that the financial data disclosed is consistent, accurate, reliable, and searchable. Implementation of the DATA Act is another step toward increasing the transparency of government spending, creating a more data-driven government, and expanding on the financial information that is accessible to the American people.

The OMB, the Chief Financial Officers Council, and the Department of the Treasury have issued guidance¹⁸ to agencies to assist with the implementation of the DATA Act requirements,

¹⁸ See Office of Management and Budget, May 8, 2015. *Increasing Transparency of Federal Spending by Making Federal Spending Data Accessible, Searchable, and Reliable*, M-15-12. Washington, DC: OMB. See also Chief Financial Officers Council, December 4, 2015. *DATA Act Implementation and Offices for Financial Assistance Awards, Controller Alert*. Washington, DC: CFO Council. See also OMB, May 3, 2016. *Additional Guidance for DATA Act Implementation: Implementing a Data-Centric Approach for Reporting Federal Spending Information*, MPM 2016-03. Washington, DC:

including defining the initial data elements and reporting requirements that must be implemented by May 2017 in order to comply with the DATA Act. The Department will need to dedicate significant resources in FYs 2016 and 2017 to complete the implementation process and meet the mandatory deadline. However, because the Department must use existing funding resources for implementation—as well as work within the constraints of its legacy financial management system—meeting the goals of the DATA Act will be a significant challenge.

Identifying a long-term solution to replace CBS

The lack of a centralized and integrated financial management system continues to create reporting and oversight challenges for the Department—including the ability to effectively report financial data and monitor financial activity across its operating units. The Department and most of its operating units use an outdated financial management system that has become increasingly difficult to maintain, as well as a resource challenge to modify for compliance with new requirements. The Department's ability to oversee and manage Department-wide financial activities is impeded by CBS' limited functionality, high support costs, lack of system integration, and lack of centralized reporting capabilities. Thus, continued reliance on CBS is an immediate high risk for the Department—and may prevent the Department from complying with the current and future reporting requirements, including the DATA Act.

Plans are in progress to replace the CBS legacy financial management system—which is not set up for data analytics, data archiving, or enterprise data warehousing—with a new comprehensive and integrated suite of financial management and business applications that will provide these functions. However, there have been significant challenges with this project, including delays in identifying a viable federal shared service provider solution for a replacement. As a result, even though it will be costly and resource intensive to maintain CBS, the Department has plans to extend its useful life through FY 2022 by performing critical technology upgrades to remain operational and secure. In addition to the use of a federal shared-service provider, the Department's challenges also include the uncertainty of adequate funding to complete the replacement project timely.

OMB. See also U.S. Treasury Department, June 24, 2016. *DATA Act Implementation Playbook*, Version 2.0. Washington, DC: Treasury.

Departmental Strategic Goal 5: OPERATIONAL EXCELLENCE

Strengthen the Department's capacity to achieve its objectives, maximize return on program investments, and deliver quality, timely service

Achieving operational excellence is essential for the Department to achieve mission-focused objectives and maximize value to its customers. This objective focuses on the high-priority, cross-cutting initiatives that the Department's leadership believes are the most critical to mission success. Our FY 2017 *Top Management and Performance Challenges* report focuses on the following:

- continuing to implement basic information security measures and expeditiously remediate critical and high-risk vulnerabilities;
- implementing the Department's cybersecurity improvement initiatives;
- managing high-risk and sole-source contracts;
- managing and strengthening the acquisition workforce;
- improving IT controls for financial data processed on the Department's systems; and
- fostering a culture of accountability.

Continuing to implement basic information security measures and expeditiously remediate critical and high-risk vulnerabilities

Federal agencies are required¹⁹ to follow NIST's risk management framework (RMF), which includes a step to determine a system's security categorization based on the impact—high, moderate, or low—that a breach of security could have on the system's confidentiality, integrity, and availability. The RMF further requires selection and implementation of a set of security controls for a system based on its security categorization.²⁰ System owners are expected to implement all applicable security controls.

However, we continue to find deficiencies in the implementation of basic security measures, such as regularly identifying vulnerabilities, expeditiously remediating security flaws, and effectively managing access controls. This relatively small set of basic security measures is essential for improving the security posture of IT systems Department-wide.

As a result of these deficiencies, Department systems continued to face the significant risk of cyber attacks. For example, all three NOAA high- and moderate-impact systems that were compromised by an attacker in September 2014 have a history of either (a) allowing high-risk vulnerabilities to persist for more than a year—significantly beyond the Department's 30-day remediation requirement—or (b) failing to detect high-risk vulnerabilities at all.

¹⁹ See Department of Commerce National Institute of Standards and Technology, February 2004. *Standards for Security Categorization of Federal Information and Information Systems*, FIPS PUB 199. Gaithersburg, MD: NIST. See also NIST, March 2006. *Minimum Security Requirements for Federal Information and Information Systems*, FIPS PUB 200. Gaithersburg, MD: NIST; see also 40 U.S.C. § 11331 and 44 U.S.C. § 3553.

²⁰ NIST, June 5, 2014. *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, NIST SP 800-37, Rev 1. Washington, DC: NIST, 18–42.

Our Cybersecurity Act of 2015 audit also identified that the Department faces significant challenges to securing its national security systems.²¹ We found that the Department had not followed longstanding requirements for managing the security risks for some of its national security systems. After we disclosed this issue to the Department's senior management in April 2016, the Chief Information Officer appointed a senior manager to make initial determinations about what corrective actions are needed to manage these risks. Currently, the Department is making progress to mitigate the security risks.

In February 2011, OMB directed federal agencies to evaluate their technology sourcing strategy so that cloud computing options are fully considered, consistent with its Cloud First policy.²² Since then, Departmental bureaus have started using cloud computing services to support their missions. While cloud computing has the potential to significantly help the Department provide reliable and innovative services, it will be challenged to ensure that basic security measures are in place. This is underscored in our ongoing IT security work at USPTO. In our ongoing work, we have found that even though a cloud service is authorized by the Federal Risk and Authorization Management Program (FedRAMP),²³ Departmental bureaus must fulfill their shared responsibility to ensure the security of their cloud solutions.

Implementing the Department's cybersecurity improvement initiatives

In recent years, the Department has made a concerted effort to implement its enterprise cybersecurity improvement initiatives, including the enterprise security operations center (ESOC) and enterprise cybersecurity monitoring and operations (ECMO). Successful implementation of these cybersecurity initiatives is critical for the Department to enhance its capability to minimize the risk of cyber attacks.

ESOC is to provide Department-wide security situational awareness to senior Departmental and bureau managers. To meet OMB's requirement,²⁴ the Department has also designated ESOC as its principal security operations center, which will be responsible for coordinating communication with the Department of Homeland Security, U.S. Computer Emergency Readiness Team, and OMB; and sharing cybersecurity intelligence and information with the Department's bureaus. During FY 2016, the Department began to deploy ESOC's final operating capabilities. By December 2016, ESOC is expected to receive and analyze cyber security-related information covering all of the Department's bureaus.

ECMO is to provide timely information about vulnerabilities to system owners in the bureaus. Last year, we reported that the Department had made substantial progress toward implementing the ECMO initiative, but the deployment on high-impact systems was still in the

²¹ DOC OIG, August 4, 2016. *Review of IT Security Policies, Procedures, Practices, and Capabilities in Accordance with the Cybersecurity Act of 2015*, OIG-16-040-A. Washington, DC: OIG.

²² Federal Cloud Computing Strategy, OMB, February 8, 2011.

²³ FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

²⁴ OMB, October 30, 2015. *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, M-16-04. Washington, DC: OMB, 16.

planning stage. Since then, the Department developed a plan to implement ECMO on its high-impact systems by October 2016.

Both ESOC and ECMO have been funded through the Department's working capital fund (WCF). This year, the amount of NOAA's contribution to the Department's WCF was limited to \$43 million, approximately \$20 million less than originally requested. As a result, the Department put the implementation of ECMO on hold until July, when its WCF received additional funding. This action could delay implementation of ECMO's ability to provide vulnerability information for high-impact systems to ESOC, thus limiting ESOC's ability to provide comprehensive situational awareness. Currently, the Department plans to complete the implementation of ECMO on high-impact systems by the end of September 2017.

Continuing the implementation of ESOC and ECMO is critical to providing timely cyber situational awareness across the Department. Accordingly, the Department needs to make the required management commitment and prioritize resources to fully implement these cybersecurity initiatives.

Managing high-risk and noncompetitive contracts

Over the years, our audit work has identified opportunities for the Department to improve its management of high-risk cost reimbursable type contracts—and save taxpayer dollars.²⁵ A government-wide initiative notes that “excessive reliance by executive agencies on sole-source contracts (or contracts with a limited number of sources) and cost-reimbursement contracts [e.g., time-and-materials and labor-hour and cost-plus] creates a risk that taxpayer funds will be spent on contracts that are wasteful, inefficient, subject to misuse, or otherwise not well designed to serve the needs of the Federal Government or the interests of the American taxpayer.”²⁶ The Department still faces challenges in contract oversight and administration of such contracts, as well as noncompetitive (i.e., no or limited competition) contracts.

For example, in a report issued in June 2016, we found that USPTO contracting and program officials did not follow best practices—Office of Federal Procurement Policy, Federal Acquisition Regulation (FAR), the Commerce Acquisition Manual, and relevant USPTO policies—for justifying and awarding noncompetitive contracts and task orders. USPTO did not adequately justify sole source contracts. We determined that USPTO did not have adequate acquisition planning processes in place, both to leverage competition as well as assure that it received fair and reasonable prices.²⁷ Our work across the Department continues to identify

²⁵ See DOC OIG, December 3, 2014. *The U.S. Patent and Trademark Office's Awarding and Administering of Time-and-Materials and Labor-Hour Contracts Needs Improvement*, OIG-15-012-A. Washington, DC: OIG. See also DOC OIG, November 8, 2013. *The Department's Awarding and Administering of Time-and-Materials and Labor-Hours Contracts Needs Improvement*, OIG-14-001-A. Washington, DC: OIG. See also DOC OIG, May 18, 2012. *NOAA's Cost-Plus-Award-Fee and Award-Term Processes Need to Support Fees and Extensions*, OIG-12-027-A. Washington, DC: OIG.

²⁶ The White House Office of the Press Secretary, March 4, 2009. “Government Contracting,” Memorandum for the Heads of Executive Departments and Agencies [online]. <https://www.whitehouse.gov/the-press-office/memorandum-heads-executive-departments-and-agencies-subject-government-contracting> (accessed August 12, 2016).

²⁷ See DOC OIG, June 16, 2016. *Awarding of U.S. Patent and Trademark Office Noncompetitive Contracts Did Not Consistently Follow Guidelines and Best Practices*, OIG-16-033-A. Washington, DC: OIG.

that—without sound procurement practices and an effective acquisition structure in place—the risk of wasted government dollars increases.

Managing and strengthening the acquisition workforce

In a September 3, 2013 memorandum, the Office of Federal Procurement Policy’s Administrator acknowledged that the federal government needs talented and trained individuals who can plan, manage, and oversee acquisitions.²⁸ During FY 2015, the Department achieved significant human capital accomplishments in managing and strengthening the acquisition workforce by enhancing recruitment efforts through attendance at college and job fairs; and utilizing the Pathways Program and other recruitment and retention incentives such as tuition assistance and loan repayment.

Although the Department fell short of its FY 2015 projected total staffing goal of 262, its recruitment effort resulted in the Department hiring 47 acquisition professionals (GS-1102 series). In addition, the Department reduced its attrition rate for GS-1102 positions by 5 percent—from 20 percent in FY 2014 to 15 percent in FY 2015.

Despite the Department’s recruitment and hiring efforts, it faces some critical challenges in managing its acquisition workforce. The first challenge is the Department’s ability to attract and retain experienced acquisition professionals to work in a location outside the Washington, DC, metropolitan area. Also, the scarcity of talent with the technical expertise and/or program management skills to manage large complex IT programs can be attributed to the fact that the pay scale and incentives in the federal government are not competitive with the private sector IT industry. Finally, budget cuts that reduced training funds, a legislative hiring cap that limits the number of employees hired within some operating units, and limited career development and advancement opportunities are continuous obstacles the Department faces in acquiring such talent.

Although the Department has established goals to overcome these challenges, it needs to continue its aggressive recruitment and hiring efforts to attract and retain the best qualified acquisition workforce at entry- and mid-level positions.

Improving IT controls for financial data processed on the Department’s systems

Maintaining effective IT controls over financial data has been a long-standing challenge for the Department. The independent auditor of the Department’s annual financial statements reported general IT controls as a Department-wide significant deficiency in FYs 2012–2015. Specifically, the Department’s financial systems continue to have deficiencies in the areas of access controls, configuration management, and segregation of duties within their financial management system. In addition, a significant deficiency related to IT access and configuration management control weaknesses was identified in the USPTO’s annual financial statement audit in FY 2015. These are substantial weaknesses that require management’s attention.

²⁸ See Office of Federal Procurement Policy, September 3, 2013, “Increasing Efficiencies in the Training, Development, and Management of the Acquisition Workforce.”

As a result, the Department and USPTO have ongoing efforts in place to implement corrective actions for the deficiencies identified. It is essential that the Department focus on improvements in these IT control areas, to ensure that the financial data processed on the Department's systems is securely maintained, has integrity, and is only available to authorized users.

Creating a Department-wide culture of accountability

Deterring, detecting, and addressing time and attendance abuse. In 2016, OIG conducted several investigations into time and attendance abuse by employees, with significant findings in operating units across the Department. This concern is not limited to one operating unit, as we have investigated issues at Census, USPTO, and NOAA, as well as referred some instances back to other bureaus for appropriate action.

Ensuring integrity in procurement processes. Over the past 3 fiscal years, OIG conducted multiple investigations into allegations of abuse in contracting matters. Some of these investigations identified practices in the Department and its components that appear inconsistent with the FAR and Department policies. For example, our investigations have uncovered inadequate justifications for sole-source awards, business practices that lend themselves to conflicts of interests—such as government officials failing to conduct market research, determine their own requirements, or develop independent government cost estimates—and contracting officers creating the appearance of impropriety by recruiting personal associates and former work colleagues for contractor positions. Our investigations have also disclosed criminal conduct in procurement, as was clearly illustrated by the recent indictment of a former Bureau of Industry and Security (BIS) employee on charges of conspiracy and bribery related to government contracts. The Department should take steps to ensure that contracts are awarded properly and in compliance with relevant law and policy, paying particular attention to high-risk acquisitions and sole-source contracts.

Preventing travel abuse. In FY 2016, OIG investigated alleged abuses related to official Department travel. These inquiries raised concerns about the Department's compliance with governing laws and rules, particularly the Federal Travel Regulation and the Department's travel-related policies. Two investigations in particular identified issues with Department personnel involved in the preparation and approval of official travel, specifically with regard to premium-class travel involving senior Department personnel. While some of the problems identified in these inquiries appeared to result from intentional abuse, other failures stemmed from critical misunderstandings of key travel-related laws and rules by one or more employees responsible for administering travel.

Appendix A: Related OIG Publications

This list presents OIG's FY 2016 work related to top management and performance challenges facing the Department in FY 2017. These products can be viewed at www.oig.doc.gov. If the product contains information that cannot be released publicly, a redacted version or an abstract will be available on the website.

Challenge 1: Trade and Investment

- *Complying with Uniform Guidance on Profit or Management Fees Under Federal Assistance Awards* (OIG-16-013-M; January 4, 2016)
- *Full Transition to the Nation's Single Export Licensing System Is Uncertain* (OIG-16-037-A; July 5, 2016)
- *CS China Operations Highlight Need to Strengthen ITA Management Controls* (OIG-16-041-A; August 9, 2016)

Challenge 2: Innovation

- *Broadband Technology Opportunities Program Recipients Retaining Excess Equipment at End of Projects* (OIG-16-012-A; December 18, 2015)
- *Audit of FirstNet's Efforts to Include Federal Agencies in its NPSBN* (OIG-16-017-A; February 8, 2016)
- *Audit of Trademark's Activity-Based Information System* (OIG-16-020-A; February 23, 2016)
- *OIG Testimony on Ongoing Activities and Challenges Facing the First Responder Network Authority in their Establishment of a Nationwide Public Safety Broadband Network* (OIG-16-034-T; June 21, 2016)
- *FirstNet Can Strengthen Its Controls by Documenting Procedures to Close and Track Interagency Agreements* (OIG-16-035-A; June 29, 2016)
- *USPTO Should Improve Controls Related to Equipment Used by Full-Time Teleworkers* (OIG-16-039-A; August 2, 2016)
- *USPTO Needs to Improve Assessment of Attaché Program Performance* (OIG-16-042-A; August 23, 2016)
- *Review of the Sustainability of Broadband Technology Opportunity Program Comprehensive Community Infrastructure Awards* (OIG-16-047-I; September 29, 2016)

Challenge 3: Environment

- *Audit of NOAA Hurricane Sandy Disaster Relief Funds* (OIG-16-014-M; January 6, 2016)
- *NOAA Fisheries Needs to Improve Management and Oversight of Electronic Monitoring Programs* (OIG-16-022-I; March 2, 2016)
- *The Joint Polar Satellite System: Further Planning and Executive Decisions Are Needed to Establish a Long-term, Robust Program* (OIG-16-026-I; April 26, 2016)

- *NOAA Fisheries' Alaska Regional Office Use of Contract Raises Issues Regarding Personal Services* (OIG-16-030-I; June 1, 2016)
- *Deputy IG Letter to Senator Rubio re: Red Snapper in South Atlantic Federal Waters* (OIG-16-044-M; August 29, 2016)
- *Deputy IG Letter to Senator Blumenthal, Senator Murphy, and Representative Courtney re: Fishing Management Across the Northeast and Mid-Atlantic* (OIG-16-045-M; September 14, 2016)
- *Delinquency Follow-Up Procedures and System Shortcomings Pose Risks for Fisheries Finance Program* (OIG-16-046-A; September 26, 2016)

Challenge 4: Data

- *Census Bureau Realignment Did Not Fully Meet Stated Goals and Reimbursable Agreements Are Not Managed Adequately* (OIG-16-004-A; October 22, 2015)
- *The U.S. Census Bureau's Efforts to Ensure an Accurate Address List Raise Concerns over Design and Lack of Cost-Benefit Analysis* (OIG-16-018-A; February 23, 2016)
- *The U.S. Census Bureau Geography Division Lacks Complete Information for Project Costs and Has Not Fully Monitored GSS-I Goals* (OIG-16-029-A; May 23, 2016)
- *2020 Census: The Bureau Has Not Reported Test Results and Executed an Inadequately Designed 2015 Test* (OIG-16-032-A; June 7, 2016)
- *OIG Testimony on The Census Bureau's Modernization Efforts and Overall Preparedness for the 2020 Census* (OIG-16-038-T; June 9, 2016)

Challenge 5: Operational Excellence

- *Significant Firm-Fixed-Price Contract Actions in FYs 2011–2013 Cannot Be Verified from Documentation in NIST Contract Files* (OIG-16-001-A; October 2, 2015)
- *Lack of Basic Security Practices Hindered BIS' Continuous Monitoring Program and Placed Critical Systems at Risk* (OIG-16-003-A; October 16, 2015)
- *FY 2015 Financial Statements Audit (USPTO)* (OIG-16-006-A; November 13, 2015)
- *FY 2015 Consolidated Financial Statements Audit (Department of Commerce)* (OIG-16-007-A; November 13, 2015)
- *2016 Annual Letter to OMB re: Government Charge Card Abuse Prevention Act of 2012* (OIG-16-016-M; January 29, 2016)
- *Census Bureau Reviews of Unliquidated Obligations Could Be Improved with Greater Review Frequency and Additional Documentation* (OIG-16-019-A; February 23, 2016)
- *NIST Working Capital Fund Budgetary Controls Are in Place but Issues with Carryover Balances Policies, and Time Charges Should be Addressed* (OIG-16-023-A; March 23, 2016)
- *NIST Must Strengthen Justifications for Remaining ULOs and Review Procedures* (OIG-16-024-A; March 24, 2016)

- *The Census Working Capital Fund Lacks Transparency* (OIG-16-025-A; April 18, 2016)
- *FY 2015 Compliance with Improper Payment Requirements* (OIG-16-027-I; May 11, 2016)
- *Awarding of U.S. Patent and Trademark Office Noncompetitive Contracts Did Not Consistently Follow Guidelines and Best Practices* (OIG-16-033-A; June 16, 2016)
- *Review of National Oceanic and Atmospheric Administration's Sole-Source Contract Awarded to Industrial Economics, Inc. Regarding Gulf Oil Spill Expert Services* (OIG-16-036-I; July 5, 2016)
- *Review of IT Security Policies, Procedures, Practices, and Capabilities in Accordance with the Cybersecurity Act of 2015* (OIG-16-040-A; August 4, 2016)
- *Successful Cyber Attack Highlights Longstanding Deficiencies in NOAA's IT Security Program* (OIG-16-043-A; August 26, 2016)
- *Analysis of Patent Examiners' Time and Attendance* (14-0990; August 31, 2016)
- *Investigation into Travel & Other Improprieties in the Office of a Politically Appointed Official* (15-0444; September 8, 2016)
- *Follow-up Audit on Recommendations from Audit Report No. OIG-13-031-A, Classified Information Policies and Practices at the Department of Commerce Need Improvement* (OIG-048-A; September 30, 2016)

Appendix B: List of Acronyms

ATMS	Advanced Technology Microwave Sounder
BIS	Bureau of Industry and Security
C.F.R.	Code of Federal Regulations
CBS	Commerce Business System
CEDCaP	Census Enterprise Data Collection and Processing System
COTS	commercial off-the-shelf
DATA Act	Digital Accountability and Transparency Act of 2014
DOC	Department of Commerce
ECMO	enterprise cybersecurity monitoring and operations
EDA	Economic Development Administration
EPQI	Enhanced Patent Quality Initiative
ESOC	enterprise security operations center
FAR	Federal Acquisition Regulation
FedRAMP	Federal Risk and Authorization Management Program
FirstNet	First Responder Network Authority
FSMS	Federal Spectrum Management System
FY	fiscal year
GOES-R	Geostationary Operational Environmental Satellite-R Series
GOES-S	Geostationary Operational Environmental Satellite-S Series
GOL	Grants Online
IAA	interagency agreement
IT	information technology
JPSS	Joint Polar Satellite System
LOA	Licensing Officer Access
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
NOAA Fisheries	NOAA National Marine Fisheries Service
NPSBN	nationwide public safety broadband network
NRFU	nonresponse followup
NTIA	National Telecommunications and Information Administration
OIG	Office of Inspector General
OMB	Office of Management and Budget
R&D	research and development
RFP	request for proposals
RMF	risk management framework
SLIGP	State and Local Implementation Grant Program
U.S.C.	United States Code
USPTO	U.S. Patent and Trademark Office
WCF	working capital fund