Top Management and Performance Challenges Facing the Department of Commerce

UNITED STATES DEPARTMENT OF COMMERCE
The Inspector General
Washington, D.C. 20230

September 29, 2017

INFORMATION MEMORANDUM FOR SECRETARY ROSS

FROM: Peggy E. Gustafson

SUBJECT: *Top Management and Performance Challenges Facing the Department of Commerce in Fiscal Year 2018*

The Office of Inspector General is required by statute[1] to report annually the most serious management and performance challenges facing the Department of Commerce. Attached is our final report on the Department's top management and performance challenges for fiscal year (FY) 2018.

The top management and performance challenges we reported on last year remain critical issues facing the Department. However, we have revised our discussion to reflect the Department's progress, changing priorities, and emerging risks.

For each challenge identified within this memorandum, please find brief descriptions of the issues discussed in greater detail in the report:

Challenge 1: Delivering a Timely 2020 Census That Maintains or Improves Data Quality but Costs Less Per Household Than the 2010 Census

- Maintaining Bureau leadership continuity to ensure that a reengineered, cost-effective decennial census occurs on schedule and produces quality results

- Developing an accurate 2020 Census life-cycle cost estimate that can be validated by stakeholders

- Implementing new, reengineered processes and systems in time to perform as needed

---

[1] 31 U.S.C. § 3516(d).

Challenge 2: Ensuring the Continuity of Environmental Satellite Observations

- Transitioning Geostationary Operational Environmental Satellite –16 and Joint Polar Satellite System–1 into operations

- Managing risk in the acquisition and development of the next-in-series satellites

- Revising Polar Follow-On program baselines in accordance with the Administration's priorities

- Assessing the viability of using commercial data in weather forecasts

Challenge 3: Securing Department Systems and Information

- Continuing security improvements for the Department's national security systems

- Ensuring security controls are effectively implemented and conducting high-quality security control assessments

- Securing cloud-based systems

- Implementing multi-factor authentication for all privileged users

- Implementing a cohesive approach to cybersecurity across the Department

Challenge 4: Deploying a Nationwide Public Safety Broadband Network (NPSBN)

- Deploying and ensuring the sustainability of the NPSBN

- Ensuring the successful performance of the contract awarded to AT&T

- Maximizing state opt-ins and participant subscriptions

- Strengthening operational controls

Challenge 5: Efficiently and Effectively Enforcing Laws That Promote Fair and Secure Trade

- Enhancing U.S. economic competitiveness through efficient administration of trade enforcement remedies and effective export promotion activities

- Facilitating U.S. exports by implementing export control reform changes while enhancing enforcement

Challenge 6: Modernizing the Department's Legacy IT Systems and Improving Data Quality

- Identifying a long-term solution to replace Commerce Business Solutions

- Transitioning the U.S. Patent and Trademark Office from legacy to next-generation IT systems

- Maintaining current, accurate, and complete data to effectively manage real property

Challenge 7: Implementing Processes to Improve Management of the Department's Contracts, Grants, and Cooperative Agreements

- Strengthening processes to govern the appropriate use of non-competitive contracts and maximize the use of competition

- Developing and maintaining a competent acquisition workforce to support the Department's mission

- Improving oversight and monitoring of Minority Business Centers to ensure accurate reporting of program goals and efficient use of program funds

- Fostering high ethical standards throughout the Department and its contracting programs to maintain the public trust

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 will be included in the Department's *Annual Financial Report*, as required by law.

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: Ellen Herbst, Chief Financial Officer/Assistant Secretary of Administration, Performing the Non-Exclusive Duties of the Deputy Secretary
Peter Davidson, General Counsel
Michelle McClelland, Deputy General Counsel
Rod Turk, Acting Chief Information Officer
Lisa Casias, Acting Chief Financial Officer/Assistant Secretary of Administration
Wendy Teramoto, Chief of Staff to the Secretary
Operating Unit Heads
Operating Unit Audit Liaisons

Contents

Cover: Herbert C. Hoover Building main entrance at 14th Street Northwest in Washington, DC. Completed in 1932, the building is named after the former Secretary of Commerce and 31st President of the United States.

Challenge 1: Delivering a Timely 2020 Census That Maintains or Improves Data Quality but Costs Less Per Household Than the 2010 Census

Early this decade, the Census Bureau committed to conducting the 2020 Census at a lower cost per household (adjusted for inflation)—while continuing to maintain high quality—than the last decennial, to end decades of rising costs. Over the past three decennial censuses, the per-household cost had climbed from approximates of $45 in 1990 and $80 in 2000 to $92 in 2010 (in 2020 constant dollars).[1] To stop these escalating costs, the Bureau estimated that it could avoid $5.2 billion in 2020 Census costs (compared with repeating the 2010 design in 2020) through major cost saving innovations in its operational design.

However, as this decade progressed, the Bureau has scaled back its cost avoidance projections. Our audit work has identified that the 2020 Census life-cycle cost estimate is not auditable, and the Bureau failed to capture information during research and testing that could help update or assess the accuracy of the estimate. Unaccounted-for costs and cost overruns have affected the address canvassing operation, information technology development, and other areas—leading the Bureau recently to reduce its cost avoidance estimate.

This challenge focuses on the following areas for management attention:

- Maintaining Bureau leadership continuity to ensure that a reengineered, cost-effective decennial census occurs on schedule and produces quality results

- Developing an accurate 2020 Census life-cycle cost estimate that can be validated by stakeholders

- Implementing new, reengineered processes and systems in time to perform as needed

Maintaining Bureau leadership continuity to ensure that a reengineered, cost-effective decennial census occurs on schedule and produces quality results

The 2020 Census's mission is to count everyone in the U.S. only once, and in the right place. The Bureau must complete its 35 separate, but interrelated, operations effectively and efficiently to achieve its mission—while conducting the decennial census at a lower cost (per household and adjusted for inflation) than the 2010 Census without sacrificing data quality. This decade, the Bureau will rely more heavily than ever on automated systems and electronic data collection by implementing operational design changes in four key areas: (1) reengineering address canvassing; (2) optimizing self-response; (3) using administrative records and third-party data; and (4) reengineering filed operations.

Considering that the Bureau is attempting to implement a redesigned decennial census at a lower cost—per household—than the 2010 Census, continuity of leadership at all levels of the organization is critical. However, the former Director, who began his term in August 2013, retired on June 30, 2017. Because the Census Bureau Director is a Presidential appointee, there

---

[1] Census Bureau, September 2016. *2020 Census Operational Plan: A New Design for the 21st Century (Version 2.0),* p. 7.

is a likelihood that the Director position will remain vacant for some time, given the inevitable delay involved in nominating and gaining confirmation of a new Director. Unfortunately, the Deputy Director position has remained vacant since January 2017, and it should be noted that key program management positions have also experienced turnover.

With some early 2020 Census operations underway—as well as the 2018 End-to-End Test, which is the culmination of the Bureau's research and its only opportunity to test nearly all major components of the 2020 Census—time is running out for a new Director to lead and guide the next decennial census to a successful outcome. We believe that filling the top two Census Bureau positions should be a high priority for the Secretary and Congress.

Developing an accurate 2020 Census life-cycle cost estimate that can be validated by stakeholders

The 2020 Census life-cycle cost estimate (LCCE) is not auditable

More than 100 variables (such as leasing costs and self-response rate) will drive the cost of the 2020 Census. However, in our report on the 2014 Census Test,[2] we found that the 2020 Census life-cycle cost estimate was not auditable. The Bureau neither obtained nor required supporting documentation for cost estimate input factors; further, it could not identify the subject matter experts who provided the inputs; or provide the rationale for each input decision.

However, efforts to improve the life-cycle cost estimate are under way. The Bureau has started linking documentation to the variables in its estimate. And, recently, the Secretary of Commerce established a task force consisting of staff from the Office of the Secretary, Office of Management and Budget, and outside consultants to identify cost overruns and review current and future budget projections. The task force is working closely with the Bureau to improve the life-cycle cost estimate and we are looking forward to reviewing the final product.

Census tests failed to capture cost data

On three occasions the Bureau's tests failed to capture cost data that could be used to validate and update the 2020 Census LCCE:

- First, although the 2014 Census Test plan indicated that cost comparison was a component of the test, the data were not collected during the test itself.

- Next, the Bureau's Address Validation Field Test (September 2014 through January 2015) sought to determine the feasibility, impact on data quality, and cost effectiveness of canvassing parts of blocks rather than entire blocks. Again, no cost data were collected.[3]

---

[2] 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: DOC OIG.

[3] DOC OIG, February 23, 2016. *The U.S. Census Bureau's Efforts to Ensure an Accurate Address List Raise Concerns over Design and Lack of Cost-Benefit Analysis*, OIG-16-018-A. Washington, DC: DOC OIG.

- Finally, the 2015 Census Test did not distinguish between the costs associated with administrative functions—most notably the differences between the labor-intensive paper payroll process and the electronic process. Therefore, the Bureau cannot determine whether greater efficiency occurred due to reengineered enumeration processes or simply because of reduced administrative burden.[4]

The Bureau has accounting weaknesses

To make informed 2020 Census design decisions, the Bureau must know how much its operations actually cost. In 2014, we found significant deficiencies in the Decennial Program's method for recording salary costs.[5] The Bureau was charging employee salary costs to projects based on predetermined budget allocations—not on actual hours worked. In addition, those recorded salary costs did not necessarily account for what the employee actually worked on. Since our report was issued, the Bureau has taken steps to ensure employees are correctly recording their time.

Some costs are not accounted for in the 2020 Census LCCE

In our 2017 audit of the Bureau's Address Canvassing Test,[6] we observed substantial cost overruns that are not reflected in the 2020 Census LCCE. Further, our evaluation of the 2016 Census Test identified nonresponse followup (NRFU) costs that are also not accounted for in the 2020 Census LCCE. To reduce 2020 Census address canvassing costs, the Bureau has elected to conduct 100 percent in-office address canvassing—which, in the 2015 version of the 2020 Census LCCE was to cost $44 million. However, during our review of this operation, we found that it would have cost at least $125 million (almost triple the estimate) from fiscal years (FYs) 2016 to 2019.[7] Citing funding uncertainties, the Bureau has since suspended a portion of the operation until 2021.

Finally, the Bureau increased the expected in-field address canvassing workload of housing units by 20 percent.[8] The precise cost impact of this is unknown. But the Bureau originally expected reengineered address canvassing to account for $900 million of its 2020 Census cost avoidance,[9] so a 20 percent increase in the in-field address canvassing workload will likely reduce the magnitude of cost avoidance the Bureau will achieve by reengineering the address canvassing operation.

---

[4] 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: DOC OIG.

[5] DOC OIG, May 21, 2014. *The Census Bureau Lacks Accurate and Informative Cost Data to Guide 2020 Census Research Through a Constrained Budget Environment*, OIG-14-021-A. Washington, DC: DOC OIG.

[6] DOC OIG, May 11, 2017. *2020 Census: The Address Canvassing Test Revealed Cost and Schedule Risks and May Not Inform Future Planning as Intended*, OIG-17-024-A. Washington, DC: DOC OIG.

[7] *Ibid.*

[8] By increasing the expected in-field address canvassing workload from 25 to 30 percent of housing units, the Bureau should see a 20 percent increase from its original estimated workload. See DOC OIG, May 11, 2017. *2020 Census: The Address Canvassing Test Revealed Cost and Schedule Risks and May Not Inform Future Planning as Intended*, OIG-17-024-A. Washington, DC: DOC OIG.

[9] *Ibid.*

The 2020 Census LCCE assumes that (1) all non-responsive housing units receive a maximum of six contact attempts and (2) all housing units will be enumerated by the sixth attempt. The 2016 Census Test was intended to test these assumptions. However, during the 2016 test, we found that the operational control system did not limit enumerators to six attempts per housing unit; rather, it limited each housing unit to six days' of attempts.[10] As a result, during the test, 10 percent of housing units received more than six attempts, resulting in more than 29,000 additional contact attempts across just 144,000 cases. When extrapolated to a potential 2020 Census NRFU workload, the LCCE may fail to account for more than 11 million NRFU contact attempts.

During recent tests, a high percentage of NRFU cases have gone "unresolved," meaning that an enumerator was unable to collect data for (or enumerate the people living in) that housing unit during the NRFU operation (see figure 1).[11] Given that the Bureau did not implement strategies to increase the response rate (e.g., nationwide publicity, the Census Partnership Program, and paid advertising) during its 2020 Census tests, this may not be a concern. However, if the trend continues—as observed in the tests—the Bureau will have to expend additional resources not currently accounted for in the cost estimate to fulfill the Constitutional requirement to count the population.

Figure 1. 2010 Census NRFU Housing Unit Unresolved Rate Compared to the 2014, 2015, and 2016 Census Tests
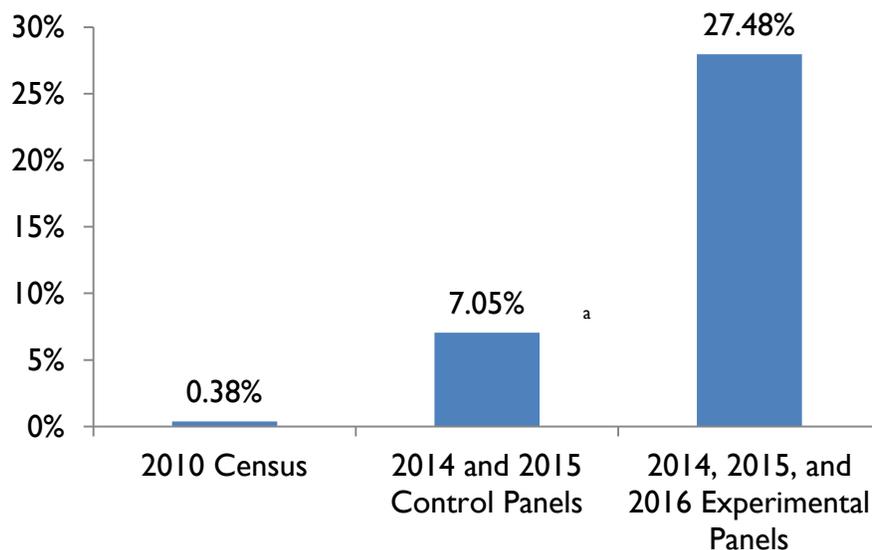
Source: U.S. Census Bureau

[a] During the 2014 and 2015 Census Tests, the Bureau made use of control panels, which conducted NRFU much the same as it was conducted during the 2010 Census in order to measure the effect on NRFU of new innovative techniques—used by experimental panels—that it is considering implementing during the 2020 Census. The 2016 Census Test did not use a control panel.

---

[10] DOC OIG, March 16, 2017. *2020 Census: 2016 Census Test Indicates the Current Life-Cycle Cost Estimate is Incomplete and Underestimates Nonresponse Followup Costs*, OIG-17-020-I. Washington, DC: DOC OIG.

[11] During the 2010 Census, the Bureau ceased NRFU operations on less than 1 percent of U.S. housing units.

The Bureau incurred cost overruns

The Bureau is in the process of revising its LCCE. Updates to several values will likely account for reduced cost avoidance numbers, including the following:

- Reduced self-response rate by 3 percent—which means increases to the NRFU workload, staff, and infrastructure needs.

- Additional early Area Census Offices (ACOs) to cover the greater-than-expected in-field address canvassing workload.

- Increased printing and postage rates due to (a) the introduction of new forms and (b) the return to a paper instrument for certain operations.

- Extra future year partnership and communication staff to accommodate current delays and resulting compressed time frame for implementation.

Additionally, the Bureau originally estimated that the Census Enterprise Data Collection and Processing (CEDCaP) program—"a bureau-wide effort that . . . creates an integrated and standardized enterprise suite of systems" that will help the Bureau successfully automate the 2020 Census—would cost $656 million (FYs 2015–2021). Then, in May 2016, the Bureau decided to use a "hybrid approach" and integrate a commercial off-the-shelf platform with select custom systems. The Bureau now estimates that the CEDCaP program will now cost $965.2 million, 47 percent more than originally estimated. If this enterprise-wide data collection solution falls short, the 2020 Census is at risk of even greater cost increases.

The Bureau has undertaken a number of major initiatives to modernize its decennial operations. Inevitably, not all 2020 Census design innovations will perform as hoped—and some potential cost avoidance may not materialize. However, for stakeholders to have any confidence in the reengineered decennial census LCCE, the Bureau must be more transparent—by documenting inputs, accurately capturing and tracking project costs, and ensuring that all relevant costs are included.

Implementing new, reengineered processes and systems in time to perform as needed

In last year's *Top Management and Performance Challenges* report, we stated that further testing of new operational design components was needed, and that the 2017 Census Test specifically was needed to collect critical information to inform the final 2020 Census operational design. Just after that report's release in September 2016, the Bureau made the decision—amid budget uncertainty—to cancel the field test portion of the 2017 test. As a result, it was unable to build on the results of the previous field tests conducted in 2014, 2015, and 2016. Perhaps even more importantly, the Bureau was unable to use the 2017 test to resolve issues—which we observed during previous tests—that limited its ability to determine the effectiveness of some of its new innovative operational design components.

During its research and testing phase, the Bureau planned to inform its 2020 Census operational design by analyzing the results of tests conducted throughout the decade. As

mentioned in greater detail in our recent reports,[12] we observed limitations to those tests that made it difficult for the Bureau to (1) make operational design decisions that are based on empirical data and (2) accurately estimate the cost of the 2020 Census. The Bureau has one final opportunity—the 2018 End-to-End Test—to test new operational design components, which it will rely on to conduct an accurate, high-quality, and cost-effective 2020 Census.

The 2018 test will include 23 of the 35 operations that comprise the 2020 Census operational design—and will be the first time testing 5 of those operations. If certain operations do not perform as expected, the Bureau will have little time to make design changes. Even if changes can be made, the Bureau may not be able to field test them before April 1, 2020 (i.e., Census Day 2020). The 2018 test has already encountered complications. Address canvassing will be field-tested at three discrete locations; however, field-testing of all enumeration activities is limited to only one location. Of particular concern is that NRFU—the largest, most expensive decennial operation—will not be adequately field-tested.

Clearly, the Bureau has taken seriously the call for a decennial census that keeps up with modern innovations. However, as the Bureau approaches Census Day 2020, many challenges remain to implement an innovative, cost-effective design. It must overcome these challenges to adequately test operational design components and make informed 2020 Census design decisions.

---

[12] *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: DOC OIG. 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: DOC OIG. Also, DOC OIG, March 16, 2017. *2020 Census: 2016 Test Indicates the Current Lifecycle Cost Estimate is Incomplete and Underestimates Nonresponse Followup Costs*, OIG-17-020-I. Washington, DC: DOC OIG. Also, DOC OIG, May 11, 2017. *2020 Census: The Address Canvassing Test Revealed Cost and Schedule Risks and May Not Inform Future Planning as Intended*, OIG-17-024-A. Washington, DC: DOC OIG.

Challenge 2: Ensuring the Continuity of Environmental Satellite Observations

National Oceanic and Atmospheric Administration (NOAA) satellite data and imagery are essential to understanding, predicting, and tracking weather and other environmental phenomena. NOAA's primary sources of these observations are satellites in geostationary and polar orbits.[13]

NOAA's constellation of Geostationary Operational Environmental Satellites (GOES) maintains a constant watch over the Western hemisphere for tracking and forecasting severe storms. On November 19, 2016, NOAA launched the first of NOAA's GOES–R series of satellites[14] with new, advanced instruments and capabilities. Upon reaching its orbit 10 days after launch, GOES–R was re-designated as GOES–16 on November 29, 2016.

Polar satellites circle above the earth from pole to pole, observing the entire globe approximately twice a day. Their data provide important input for numerical weather prediction systems' 3–7 day forecasts. Joint Polar Satellite System (JPSS) satellites,[15] which include a demonstration-turned-operational satellite known as Suomi National Polar-orbiting Partnership (NPP), fulfill NOAA's responsibility for the afternoon polar orbit.[16] JPSS–1 is anticipated to launch in November 2017, more than 6 months past its formal commitment date.

Beyond its own satellites and those of international and intergovernmental partners, NOAA is seeking to leverage capabilities in the emerging sector of commercial space services. To this end, NOAA has initiated a pilot program to assess commercially-provided environmental data.

Regarding challenges we identified in FY 2017, NOAA met some (e.g., launching GOES-R; establishing program baselines for additional JPSS missions) and had to delay others (e.g., completing its ground system and launching JPSS-1 on schedule).[17] For FY 2018, in order to mitigate the risk of gaps and ensure short- and long-term continuity of NOAA satellite data and imagery, this challenge focuses on the following areas for management attention:

- Transitioning GOES–16 and JPSS–1 into operations

- Managing risk in the acquisition and development of the next-in-series satellites

- Revising Polar Follow-On (PFO) program baselines in accordance with the Administration's priorities

- Assessing the viability of using commercial data in weather forecasts

---

[13] These include satellites owned by NOAA and domestic and international partners.

[14] This series consists of 4 satellites, GOES-R, –S, –T, and –U, which have been or will be renamed after launch.

[15] This series consists of Suomi NPP and JPSS–1, –2, –3, and –4. The JPSS-designated satellites will be renamed after launch (e.g., JPSS–1 will be renamed NOAA–20).

[16] Suomi National Polar-orbiting Partnership's (Suomi NPP's) afternoon polar orbit designation is determined by when the satellite crosses over the equator on each orbit.

[17] DOC OIG, September 30, 2016. *Top Management and Performance Challenges Facing the Department of Commerce in FY 2017*, OIG-16-049. Washington, DC: DOC OIG.

Transitioning GOES–16 and JPSS–1 into operations

GOES–16

In November 2017, after a year of testing, NOAA plans for GOES–16 to take the GOES–East position, which, according to NOAA, "offers full coverage of the continental United States and provides optimal viewing of the states and cities in the plains, mid-west and east most impacted by severe weather events including Atlantic hurricanes, thunderstorms and tornadoes, major winter storms, and flooding."[18] GOES–15 occupies the GOES–West position and NOAA maintains GOES–14 at a location in between, in storage-mode, as a back-up to respond to contingency events with the two operational satellites.

Since its launch, GOES–16 has undergone a rigorous test campaign. Importantly, the satellite's Advanced Baseline Imager has performed well. However, several issues with other components were identified that will result in reduced functionality or future performance problems. The most significant issue relates to the accuracy of its magnetometer,[19] which was promised to be two times more accurate than legacy GOES satellites. However, radio frequency interference is limiting the GOES–16 magnetometer's accuracy to the equivalent of the legacy satellites' instruments. NOAA has accepted this limitation on GOES–16 and is looking to make design changes on subsequent satellites in the series. Nevertheless, GOES–16 promises significant performance improvements over the legacy satellites once it is fully operational.

JPSS-1

In November 2016, NOAA's primary polar satellite, Suomi NPP, began operating beyond its 5-year mission design-life. With no other satellite providing JPSS-quality data, NOAA entered a period of increased risk of a gap in data from the afternoon polar orbit. With the launch of JPSS–1 in November 2017, NOAA will have passed a significant hurdle to mitigating that risk. However, the potential for a data gap will remain elevated until JPSS–1 data are sufficiently tested and then assimilated in operational forecast models. In order for JPSS–1 data to be ready for operational use, the NOAA/National Aeronautics and Space Administration (NASA) JPSS program must complete a "checkout" of the satellite and calibrate and validate the instruments and data. The program should leverage lessons learned from Suomi NPP's checkout and calibration and validation efforts.

Additionally, NOAA's National Weather Service (NWS) must perform its own experiments to ensure that JPSS–1 data provide a statistically neutral or better impact on forecast models. In order to fully assess the data, NWS planned to examine its effect for at least two seasons (i.e., 6 months) and then incorporate the data into its operational models during a routine upgrade of its systems. This process was estimated to take about 1 year from the launch of JPSS–1 but the actual timeframe will depend on the availability of data from the instruments and the results of NWS tests.

---

[18] National Oceanic and Atmospheric Administration National Environmental Satellite, Data, and Information Service, May 22–28, 2017. *GOES–R Series Program Weekly Report*. Washington, DC: NOAA.

[19] The magnetometer measures the magnetic field at the satellite's position, helping Space Weather Prediction Center forecasters to characterize the effects of solar phenomena on Earth's magnetic field.

In April 2016, we reported that NOAA intended to but had not yet developed a contingency plan for accelerating the assimilation of JPSS–1 data into its forecast models, in the event that Suomi NPP problems led to a data gap. We recommended that a contingency plan be completed and communicated to stakeholders 6 months prior to the then-planned launch date.[20] JPSS–1's launch was subsequently delayed to November 10, 2017. However, NOAA did not complete the contingency plan until September 20, 2017, and is now in the process of communicating that plan to stakeholders. In addition, NOAA had not provided stakeholders with a list of key activities for operationalizing JPSS–1 during a potential data gap in accordance with another recommendation we made.[21]

Managing risk in the acquisition and development of the next-in-series satellites

GOES–S, –T, and –U

The next satellite in the GOES–R series, GOES–S, is scheduled to launch in the second quarter of FY 2018. Prior to launch, the GOES-R Series program must make modifications to GOES–S in response to issues identified with GOES–16, posing risk to the schedule. The program must manage these issues, as well as the inherent risks in satellite integration and environmental testing. Although GOES–S has completed the bulk of its testing, an issue with the spacecraft's power regulation unit was discovered during a thermal vacuum test. This issue may delay the GOES–S schedule once the program determines the root cause and corrective action. The program must manage related issues and risks for GOES–T and –U.

In February 2017, the National Environmental Satellite, Data, and Information Service (NESDIS) delayed the planned launch of GOES–T over a year (to June 2020; GOES–U's planned launch is in April 2024). This decision came after the successful launch of GOES-R and an assessment of the health of the GOES constellation (including the anticipated launch of GOES–S in 2018). However, GOES–13 and GOES–15 (the current GOES–East and –West operational satellites) have experienced technical problems. In the past several years, GOES–13 failures have twice necessitated a call-up of the backup satellite. Additionally, GOES–15 only has one of its three star trackers available for satellite navigation. If the final star tracker fails, GOES–15 will be unable to meet its mission requirements. GOES–14 is the current on-orbit back-up satellite and from the same series as –13 and –15. While GOES–14 has not had comparable problems thus far, management must continue to pay close attention to the health of the GOES constellation and consider ramifications for the schedules of the not-yet-launched satellites.

JPSS–2, –3, and –4

The JPSS program must manage risks with development of the JPSS–2 spacecraft and instruments. The spacecraft for JPSS–2 will be different than Suomi NPP and JPSS–1 after its contract was competitively awarded to a different vendor. So far, the program has determined

---

[20] 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: DOC OIG. See finding III.A and recommendation 5.

[21] *Ibid* (see recommendation 6).

a need to customize a spacecraft electronics module and modify ground system software to interface with the new spacecraft.

Instrument acquisitions for JPSS–1 started under the JPSS predecessor program.[22] JPSS–2 instruments will be the first to be wholly acquired by this program. Given the unique instrument designs and the passage of time since the JPSS–1 development phase, the program and its contractors have in some cases needed to find new suppliers for parts or restart old production lines, which presents risks. One such issue has already materialized on a key instrument, the Cross-track Infrared Sounder, delaying its scheduled completion by 7 months.

The JPSS–2 satellite will establish the technical baseline for the JPSS–3 and JPSS–4 satellites, which will be copies of JPSS–2. Instrument acquisitions for those two missions have been initiated under block-buy procurements. Spacecraft for JPSS–3 and JPSS–4 have been negotiated as options under the JPSS–2 contract. However, NOAA's FY 2018 budget signaled a need to revise the acquisition timelines for these missions.

Revising Polar Follow-On (PFO) program baselines in accordance with the Administration's priorities

In December of 2016, the Department established cost and schedule baselines for the PFO program, which funds the JPSS–3 and JPSS–4 missions. These baselines formalized a strategy to procure the JPSS–3 and JPSS–4 satellites using a block-buy acquisition approach and were intended to make NOAA's polar satellite architecture more resilient such that two on-orbit satellites would need to fail before an actual gap in JPSS data would occur. To do this, the JPSS–3 and JPSS–4 satellites were to be completed and launch-ready well in advance of their scheduled launch dates (2 and 5 years before, respectively), so that they could launch earlier if needed to restore the on-orbit constellation to a two-failure condition (i.e., with two operational satellites). In addition, PFO plans included a JPSS–3 contingency mission, which would launch a satellite with only microwave and infrared sounders at an even earlier date if a gap condition existed.

However, NOAA's FY 2018 budget submission signaled a departure from this strategy, requesting about $180 million (i.e., only 43 percent of the almost $419 million in funds its previously-established PFO program cost baseline required for FY 2018). In the submission, NOAA proposed to continue development of the JPSS–3 and –4 missions while it re-plans the PFO program. This will involve updating its constellation availability analysis and refining its existing gap analysis to identify new launch dates, in accordance with a to-be-determined budget profile (NOAA did not provide funding estimates beyond FY 2018 in the budget submission).

Our ongoing audit work includes an assessment of the established PFO system design. We previously reported that policy, procedures, and plans for implementing the PFO "launch-on-need" strategy were among the least mature aspects.[23] However, NOAA will need to adjust

---

[22] JPSS was established in February 2010 as the civilian successor to the restructured National Polar-orbiting Operational Environmental Satellite System.

[23] 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: DOC OIG. See finding III, B.

that strategy according to the budget priorities of the Administration. Given that instrument development is typically the biggest challenge to satellite development schedules, the JPSS program will need to determine to what extent it can support the acquisition timelines of PFO instruments. Upon completion of its constellation availability and gap analyses, NOAA should inform stakeholders of the ramifications of changes to its approach for PFO, with explanations of the risks to weather forecasts and other uses of JPSS data.

Assessing the viability of using commercial data in weather forecasts

The Weather Research and Forecasting Innovation Act of 2017[24] directs NOAA to submit to Congress a strategy to enable the procurement of quality commercial weather data. It also requires NOAA to pursue pilot contracts to calibrate and evaluate commercial weather data.[25]

Before that law was enacted, NOAA had already begun efforts to assess commercial weather data. NESDIS established a Commercial Weather Data Pilot project in FY 2016. Round 1 of the project intended to assess space-based radio occultation data from two providers.[26] However, one of the providers was not able to launch its satellites and therefore did not provide data before the contracts ended on April 30, 2017. NOAA expects to complete its analysis of the collected data by the end of FY 2017 and report the results in early FY 2018.

In January 2017, NESDIS published its Commercial Space Activities Assessment Process. The document outlines three broad categories of data evaluation criteria: (1) value (of the data type to the observing system), (2) cost effectiveness (compared with data provided by government or international partners), and (3) exploitability (data formats, security, and implications of data rights for downstream use).[27]

In May 2017, NESDIS initiated round 2 of its Commercial Weather Data Pilot, which again involves the purchase and evaluation of radio occultation data, but adds operational-like requirements. NOAA intends to evaluate the data's impact on numerical weather prediction models and develop infrastructure needed for actual operational use of commercial radio occultation data.

In communications to stakeholders, NESDIS has indicated it will continue to issue requests for information to the commercial sector in efforts to identify new, emerging, or existing observing system capabilities that could meet NOAA's mission requirements. Its FY 2018 budget submission indicates ongoing and iterative purchases and assessments of commercial data over the next 5 years. However, Congress expects a report within 3 years of the results of NOAA's determination of the viability of commercial data that it has studied under pilot contracts,

---

[24] Pub. L. No. 115-25 § 301(a)(1)(B) (2017).

[25] *Id*. at § 302(c)(2).

[26] Radio occultation involves small satellites that measure distortions caused by the earth's atmosphere in radio signals sent from higher-orbiting Global Position System satellites. These measurements are used to generate "soundings" of atmospheric conditions, including temperature, pressure, density, and water vapor content.

[27] NESDIS Procedural Requirement 8010.01A, NOAA/NESDIS Commercial Space Activities Assessment Process, January 2017; 8–9.

including whether and how much the data add value to forecasts and how cost-effective it would be to obtain it for operational use.

Given that the first round of NOAA's pilot program was ultimately limited to one provider of radio occultation data, the agency, in the near-term, is likely to be challenged to obtain sufficient samples of data for analysis. Management will need to regularly inform stakeholders of the challenges stemming from the nascent commercial weather data industry and the ramifications these may have for the eventual operational use of commercial data.

Challenge 3: Securing Department Systems and Information

Over the past 5 years, previous versions of our *Top Management and Performance Challenges Facing the Department of Commerce* report have encouraged the Department to continually improve the effectiveness of its security measures protecting the confidentiality, integrity, and availability of critical systems and information. However, our recent and ongoing audits confirm that the Department continues to encounter serious challenges to securing its critical systems, including national security systems. Furthermore, persistent security weaknesses with implementing basic security controls and measures significantly increase the likelihood of system and information compromise. Given these considerations, this challenge focuses on the following cybersecurity areas for immediate management attention:

- Continuing security improvements for the Department's national security systems

- Ensuring security controls are effectively implemented and conducting high-quality security control assessments

- Securing cloud-based systems

- Implementing multi-factor authentication for all privileged users

- Implementing a cohesive approach to cybersecurity across the Department

Continuing security improvements for the Department's national security systems

Our work in FY 2016 related to the Cybersecurity Act of 2015 identified that the Department faced significant challenges to securing its national security systems. The Department has taken steps to strengthen its IT security program by revising security policy, assigning new system management, and conducting security assessments. While the Department has made progress in addressing the issues we identified, it must continue to maintain management oversight to ensure that appropriate security is implemented and maintained for these critical systems.

Ensuring security controls are effectively implemented and conducting high-quality security control assessments

According to the National Institute of Standards and Technology (NIST), system security plans should describe how each security control employed within an information system is being implemented or planned to be implemented.[28] These control descriptions should provide sufficient information for implementing the control in its operational environment as well as assessing the effectiveness of implementation. System security plans also should accurately convey how each security control will meet defined control requirements—and security assessments should effectively evaluate the resulting control implementation in order to identify vulnerabilities and present a realistic picture of the system's security posture.

Our 2016 Federal Information Security Modernization Act audit work found that the system security plans for the systems we reviewed did not adequately describe how the security

---

[28] NIST, February 2006. *Guide for Developing Security Plans for Federal Information Systems*, NIST SP 800-18, Rev 1. Gaithersburg, MD: NIST.

controls were employed within the system. Furthermore, we found that security control assessments for those systems were not conducted with sufficient rigor to determine whether controls were implemented correctly. For example, we found that assessments did not evaluate all control requirements, did not provide appropriate evidence to confirm assessment results, and did not use appropriate methods to assess technical controls.

More recently, our ongoing cybersecurity audit work is revealing problems with assessing and implementing security control on Department systems, including those supporting the 2020 decennial census.

Securing cloud-based systems

The use of commercial cloud services allows the Department to leverage a vast pool of computing resources. However, when leveraging a cloud service, the customer retains a level of responsibility to implement security measures for the cloud-based system. We have found that the Department has misunderstood security responsibilities for cloud-based systems—leading operating units (OUs) to incorrectly rely on the cloud service provider (CSP) to implement security and leaving the security for these systems deficient. During a recent audit,[29] we found that the U.S. Patent and Trademark Office (USPTO) misplaced reliance on the CSP and thus failed to implement the required security controls for cloud-based systems.

In our ongoing work at the International Trade Administration (ITA), we have preliminarily found related issues of providing security for cloud-based systems. These challenges illustrate the need to increase the awareness of security responsibilities for commercial cloud services used by the Department and its bureaus.

Implementing multi-factor authentication for all privileged users

The Department needs to make implementation of multi-factor authentication[30] for privileged users across the Department a priority. As part of our work in FY 2016,[31] we found that multi-factor authentication for users within the Department had not been fully implemented. This issue has been considered a major contributing factor to the success of several high profile cyber-attacks within the federal government (such as the major breach of personnel records at the U.S. Office of Personnel Management). Our work last year[32] also found that a major cybersecurity attack that had been successfully staged against NOAA could have been significantly reduced had multi-factor authentication been fully implemented within the NOAA systems attacked. While the Department is reporting significant progress toward fully

---

[29] DOC OIG, March 24, 2017. *Inadequate Security Practices, Including Impaired Security of Cloud Services, Undermine USPTO's IT Security Posture*, OIG-17-021-A. Washington DC: DOC OIG.

[30] Multi-factor authentication requires using two or more factors to verify the identity of a user, process, or device as a prerequisite to allowing access to resources in an information system. Factors include: (i) something a user knows (e.g. password/PIN); (ii) something a user has (e.g., cryptographic identification device, token); or (iii) something a user is (e.g., biometric).

[31] 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: DOC OIG.

[32] DOC OIG, August 26, 2016. *Successful Cyber Attack Highlights Longstanding Deficiencies in NOAA's IT Security Program*, OIG-16-043-A. Washington DC: DOC OIG.

implementing multi-factor authentication by the end of FY 2017, the Department should focus on any systems still needing to implement multi-factor authentication for privileged users.

Implementing a cohesive approach to cybersecurity across the Department

In order to implement a cohesive approach to cybersecurity across the Department, OUs need to take full advantage of available enterprise security services and implement security measures based on up-to-date policies and procedures.

Fully utilizing the Department's enterprise security services at each bureau

The Department has developed enterprise services for continuous monitoring and incident response. The Enterprise Security Operations Center (ESOC) provides access to threat indicators and intelligence that is being responded to across OUs. In our review of the Department's implementation of the Cybersecurity Information Sharing Act of 2015,[33] we found that—while ESOC has visibility into all OUs—it is a challenge for security personnel within the OUs to access the information being shared. Specifically, because a variety of security tools are used within OUs, effective integration of ESOC services with existing OU security programs has been slow. Further, the Department has been implementing the Enterprise Cybersecurity Monitoring and Operations (ECMO) program—to provide timely information about vulnerabilities to system owners in the bureaus—since 2014. However, in August 2017, the Department reported that OUs are still not fully utilizing ECMO capabilities. In order for a more efficient and cohesive IT security program to be implemented across the entire Department, the bureaus should make full use of the Department's enterprise security services, including ESOC and ECMO tools.

Prioritizing the updating of IT security policies and procedures

Due to the federated nature of the Department's bureaus and the authority of OUs' chief information officers, Department-wide policy initiatives can present challenges and are in need of updates. Policy updates have been neglected; for example, the Risk Management Framework policy[34] was issued in 2012 and has not been updated to align with NIST SP 800-53 revision 4,[35] despite the requirement to comply with this NIST standard since April 2014.[36] While the Department developed a schedule for updating and issuing new enterprise policies and minimum standards in FYs 2017 and 2018, the Department is poorly positioned to implement the upcoming NIST SP 800-53 revision 5,[37] which will likely include significant changes for implementing security controls. The Department's outdated cybersecurity-related policies

---

[33] Pub. L. No. 114-113, 129 Stat. 2242, 2936 (2015); 6 U.S.C § 1501 et seq.

[34] Department of Commerce Chief Information Officer, July 3, 2012. *Commerce Information Technology Requirement Risk Management Framework (RMF)*, CITR-19. Washington, DC: DOC.

[35] NIST, April 2013. *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST SP 800-53, Rev 4. Gaithersburg, MD: NIST.

[36] Office of Management and Budget, November 18, 2013. *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, M-14-04. Washington, DC: OMB, 5.

[37] NIST, August 2017. *Security and Privacy Controls for Information Systems and Organizations, Draft*, NIST SP 800-53, Rev 5. Gaithersburg, MD: NIST.

provide no clear direction for OUs to adequately implement their security programs, which increases the risk of noncompliance with current federal requirements for securing information systems.

Challenge 4: Deploying a Nationwide Public Safety Broadband Network (NPSBN)

The Middle Class Tax Relief and Job Creation Act of 2012 (the Act) established the First Responder Network Authority (FirstNet) as an independent authority within the National Telecommunications and Information Administration (NTIA) to implement a Nationwide Public Safety Broadband Network (NPSBN) dedicated for first responders. Also, the Act provided funding to NTIA and NIST to support NPSBN implementation. On March 30, 2017, FirstNet selected AT&T as its partner in the development of the NPSBN. The contract will be performed over the next 25 years.

With the partnership now underway, the Department and FirstNet's immediate challenges include the following:

- Deploying and ensuring the sustainability of the NPSBN

- Ensuring the successful performance of the contract awarded to AT&T

- Maximizing state opt-ins and participant subscriptions

- Strengthening operational controls

Deploying and ensuring the sustainability of the NPSBN

FirstNet's greatest challenge is the deployment of the NPSBN through 2022 and ensuring its sustainability over the next 25 years.[38] On its website, FirstNet broadly defines its network in several distinct layers:

- *Core Network.* The core network involves switching data, processing and reformatting information, and storing, maintaining, and securing data. It will interface with other state, local, and federal networks, including 911 and the Internet, covering all 56 U.S. states, territories, and the District of Columbia.

- *Transport Backhaul.* The transport backhaul will represent "the links that carry user traffic, such as voice, data, and video, and signaling from the radio base stations to the core network."[39]

- *Radio Access Network (RAN).* The RAN portion of the network will consist of the radio base station infrastructure that connects to user devices. The RAN will include cell towers as well as mobile hotspots embedded in vehicles that backhaul to the core network over satellite or other types of wireless infrastructure.

---

[38] "As a result of the Act, FirstNet holds a single, nationwide license issued by the FCC to utilize frequencies 758.00 to 768.00 MHz and 788.00 to 798.00 MHz for the purposes of ensuring the development, deployment and operation of the NPSBN. This range of frequencies is often referred to as 'Band 14.'" See First Responders Network Authority. Band 14 Incumbent Spectrum Relocation Grant Program: Frequently Asked Questions (FAQs) [online]. https://www.firstnet.gov/sites/default/files/RelocationGrantPrgrm-FAQ_0.pdf (accessed August 14, 2017).

[39] First Responders Network Authority. *Band 14 Incumbent Spectrum Relocation Grant Program: Frequently Asked Questions (FAQs) [online]*. https://www.firstnet.gov/sites/default/files/RelocationGrantPrgrm-FAQ_0.pdf (accessed August 14, 2017).

- *Public Safety Devices.* With the potential for millions of customers, devices connecting to the NPSBN will need to be resilient, easy to use, convenient to carry, and easy to administer and secure. The NPSBN is also expected to support public safety applications and mission-critical network services for first responders and the public safety community.

FirstNet needs to be self-sustaining over its 25-year partnership with AT&T. Funds provided through the Act and generated revenue need to be sufficient to fund the construction, operation, and reinvestment in the network while securing FirstNet's solvency.

OIG is completing an audit of NTIA and the Los Angeles Regional Interoperable Communications System (LA-RICS). LA-RICS was designed to serve as one of several pilot projects representing a model of how a public safety broadband project might be designed, owned, operated, and maintained. FirstNet has worked with LA-RICS and other pilot projects to acquire and incorporate lessons learned in developing the NPSBN.

Ensuring the successful performance of the contract awarded to AT&T

Under the contract awarded to AT&T, FirstNet will provide AT&T up to $6.5 billion in payments and the exclusive use of high-value, telecommunications spectrum, in exchange for the implementation and operation of the NPSBN. The value and complexity presents significant challenges to FirstNet and the Department. Earlier OIG work on FirstNet[40] identified findings associated with contracting practices on a smaller scale. FirstNet—which has worked with the Department of Interior on its contract administration and has submitted corrective action plans to OIG to address previous findings—must now demonstrate that it has re-worked its oversight processes and can monitor a contract of this magnitude.

FirstNet employed an objectives-based approach in its request for proposal—rather than a traditional requirements-driven model throughout the NPSBN contracting process. FirstNet must now monitor AT&T performance to ensure it successfully meets the terms of the contract. With the need to develop unique solutions for each of the states and territories, FirstNet is likely to encounter numerous challenges of interest to users of the network, including the extent of rural coverage, user priority, user preemption, and network reliability. For the network to succeed, FirstNet will need to provide continuous and effective oversight of its contract with AT&T.

Maximizing state opt-ins and participant subscriptions

The heads of the 56 states, territories, and the District of Columbia will decide by the end of calendar year 2017 whether their state or territory will either opt-in (i.e., choose FirstNet to deploy a public safety broadband radio access network, the system needed to connect devices to FirstNet's nationwide network) or opt-out (i.e., choose to assume the responsibility itself). NPSBN implementation scenarios will differ widely, depending on the extent to which states opt-in to the network and on how well FirstNet and AT&T are able to entice public safety

---

[40] DOC OIG, December 5, 2014. *FirstNet Must Strengthen Management of Financial Disclosures and Monitoring of Contracts*, OIG-15-013-A. Washington, DC: DOC OIG.

organizations to purchase services. Regardless of whether a state opts in or opts out, however, public safety entities are not required to subscribe to the network. FirstNet must meet the public safety community's requirements, with services at an affordable cost.

In March 2017 we reported[41] on NTIA's management of the State and Local Implementation Grant Program (SLIGP), a program funded by the Act that supports state and territory efforts to prepare for the NPSBN in advance of each state's and territory's decision to opt-in or opt-out of the network. We found that control processes for detecting fraud, waste, and abuse were incomplete—and that NTIA did not maintain readily available assessments of each recipient's status towards achieving SLIGP priorities. NTIA submitted a responsive action plan to address these recommendations, which we will assess in oversight work related to future grant programs.

Strengthening operational controls

As a relatively new federal entity, FirstNet has experienced challenges with respect to its control environment. As noted in our prior work, FirstNet encountered multiple issues with controls over financial disclosures, monitoring of potential conflicts of interest, and human resources—in addition to contracting practices and oversight of hiring.[42] OIG also identified the need for FirstNet to strengthen its controls in areas such as hiring, outreach, and the use of interagency agreements (IAAs). In our August 2015 report,[43] we identified areas where improvements could be made with respect to FirstNet's (1) workforce and recruiting challenges, (2) participation at the discretionary outreach events, and (3) internal control. In our February 2016 report,[44] we identified opportunities to improve the effectiveness of the federal consultation program, including strengthening accountability, increasing federal input, and documenting federal agency analyses. In our June 2016 report[45] on FirstNet's use of IAAs, we identified how FirstNet controls associated with tracking IAAs and providing timely documentation to support monitoring efforts could be improved. FirstNet has taken prompt steps to address the recommendations contained within these reports, including filling many of its key positions and updating its process controls. FirstNet is encouraged to continue to take steps to strengthen its policies and controls.

FirstNet is also implementing its first grant program assisting entities that currently operate on the Band 14 range of frequencies to relocate their communications operations to other frequencies—the Band 14 Incumbent Spectrum Relocation Grant Program. OIG currently has an ongoing audit of FirstNet's management and oversight of this program.

---

[41] DOC OIG, March 14, 2017. *Expanding Monitoring Controls Will Strengthen the Management of the State and Local Implementation Grant Program (SLIGP)*, OIG-17-018-A. Washington, DC: DOC OIG.

[42] DOC OIG, December 5, 2014. *FirstNet Must Strengthen Management of Financial Disclosures and Monitoring of Contracts*, OIG-15-013-A. Washington, DC: DOC OIG.

[43] 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: DOC OIG.

[44] DOC OIG, February 8, 2016. *Audit of FirstNet's Efforts to Include Federal Agencies in its NPSBN*, OIG-16-017-A. Washington, DC: DOC OIG.

[45] 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: DOC OIG.

To remain in compliance with the Act while conducting its mission, FirstNet must also ensure that its administrative expenses do not exceed $100 million over the first 10 years of operations.[46] Adding and strengthening controls will continue to remain important as the building of nationwide network progresses and FirstNet takes on additional responsibilities.

---

[46] 47 U.S.C. § 1427(b)(1).

Challenge 5: Efficiently and Effectively Enforcing Laws That Promote Fair and Secure Trade

As the federal government's lead trade and investment promotion agency, the Department faces the challenge of helping U.S. companies be more competitive abroad and attracting foreign investment while protecting U.S. national security interests. Those missions are carried out by the International Trade Administration (ITA), which assists U.S. exporters to sell their products overseas and enforces U.S. trade laws and agreements, and the Bureau of Industry and Security (BIS), which administers and enforces U.S. export control laws and regulations. In the area of international trade, the current Administration has prioritized enforcing laws that promote fair and secure trade. A series of directives involving international trade have underscored that priority. For example, an April 29, 2017, executive order directed the Secretary, the U.S. Trade Representative, and other heads of executive departments and agencies, as appropriate, to take every appropriate and lawful action to address violations of trade law, abuses of trade law, or instances of unfair treatment.[47] Therefore, ITA and BIS must utilize their resources effectively and efficiently as they participate in government-wide efforts to ensure fair trade that protects national security.

This challenge focuses on the following areas for management attention:

- Enhancing U.S. economic competitiveness through efficient administration of trade enforcement remedies and effective export promotion activities

- Facilitating U.S. exports by implementing export control reform changes while enhancing enforcement

Enhancing U.S. economic competitiveness through efficient administration of trade enforcement remedies and effective export promotion activities

In 2017, the Department's international trade priorities shifted from trade promotion to trade enforcement. The President's FY 2018 budget justification for ITA increases funding and staff for the bureau's Enforcement and Compliance (E&C) business unit, which handles trade enforcement and compliance functions, including antidumping and countervailing duty (AD/CVD) investigations. Conversely, it reduces resources for the Global Markets (GM) and Industry and Analysis units, which primarily focus on trade promotion and trade analysis activities, respectively.[48] Specifically, the justification requests additional funding for personnel to establish a team within E&C dedicated to self-initiating investigations.[49] This contrasts with the traditional process for initiating an AD/CVD investigation, which requires a petition from an interested party, such as a company or trade association.[50]

---

[47] President, Executive Order 13796, "Addressing Trade Agreement Violations and Abuses," 82 Fed. Reg. 20819 (May 4, 2017).

[48] DOC, *International Trade Administration, Budget Estimates, Fiscal Year 2018*, Washington, DC: DOC, ITA 7 and 8.

[49] *Ibid*, ITA 35.

[50] The self-initiating and traditional processes for initiating AD/CVD investigations are set forth in the Tariff Act of 1930, as amended (19 U.S.C. §§1671a and 1673a).

Creating a new team and adding personnel to enhance E&C's capacity to self-initiate AD/CVD investigations requires additional guidance and training for new staff who may not be accustomed to conducting these cases. In our FYs 2016–2017 audit of E&C's efforts to ensure accurate and timely trade remedy determinations, we found that the office needed to update its quality assurance practices and implement them in a consistent manner across its offices.[51] E&C must ensure that its quality assurance practices apply to self-initiated cases as well.

The effective use of government funds within a rescaled ITA requires GM to focus its export promotion activities on markets with the greatest potential and to improve service delivery to clients. At present, GM operates in 122 overseas cities in 78 countries and has 108 offices in the United States. With the FY 2018 budget justification calling for the closure of an estimated 35 international and 10 domestic offices, GM will need to focus on locations in top performing markets, which will require accurate services data to make such determinations.[52]

GM's U.S. & Foreign Commercial Service (USFCS) faces the challenge of restructuring its international and domestic coverage by closing low performing offices and downsizing its workforce while ensuring management controls are in place to effectively deliver client services. Using USFCS performance data, our 2012 report identified low performing domestic offices that could be closed and would result in modest savings.[53] In our August 2016 audit of USFCS operations in China, OIG identified several management control issues inhibiting effective operations, as well as data limitations that prevented accurate assessment of service delivery quality, such as how long it takes to fulfill a client service or why participation agreements were canceled.[54]

Facilitating U.S. exports by implementing export control reform changes while enhancing enforcement

BIS has achieved a significant increase in total export license applications processed—from 24,782 in FY 2013 to 33,615 in FY 2016.[55] This is due to the export control reform initiative begun in 2010, which moved items from the U.S. Munitions List to the Commerce Control List.

With an increase in license applications comes the need to strengthen enforcement efforts to ensure exporters comply with the Export Administration Regulations (EAR). Enforcement may encompass continued proactive outreach by BIS staff, formal investigations carried out by BIS special agents, and other enforcement activities associated with the export licensing process. Former defense exporters who are new to the EAR must be educated on how BIS's regulations will affect their ability to export their products. In addition to outreach, BIS will require increased enforcement capacity to investigate leads that may eventually become active cases. In

---

[51] DOC OIG, February 28, 2017, *Enforcement and Compliance Needs to Update and Consistently Implement Its Quality Assurance Policies and Practices*, OIG-17-017-A. Washington, DC: DOC OIG.

[52] DOC, *International Trade Administration, Budget Estimates, Fiscal Year 2018*, ITA 47.

[53] DOC OIG, November 30, 2012, *U.S. Export Assistance Centers Could Improve Their Delivery of Client Services and Cost Recovery Efforts*, OIG-13-010-I. Washington, DC: DOC OIG.

[54] DOC OIG, August 9, 2016, *CS China Operations Highlight Need to Strengthen ITA Management Controls*, OIG-16-041-A. Washington, DC: DOC OIG.

[55] DOC, *Bureau of Industry and Security, Fiscal Year 2018, President Submission*, Washington, DC: Commerce, BIS 26.

FY 2016, BIS reported that it only initiated cases on slightly more than 75 percent of leads opened that same year; in FY 2015, the figure was slightly less than 60 percent.[56] BIS must ensure that it has plans in place for the effective use of additional enforcement resources as it continues to implement changes brought about by the export control reform initiative.

Finally, end-use checks are important enforcement tools that may be conducted before or after an export is made to ensure a foreign end-user complies with the terms of an export license and the EAR. Such checks may be carried out by export control officers stationed overseas, BIS special agents, and USFCS commercial officers. In FYs 2015 and 2016, BIS conducted 1,031 and 985 checks respectively—of which 3 and 4 percent were carried out by USFCS commercial officers.[57] Despite the small number of checks performed, a reduction of up to 38 USFCS commercial officer positions overseas as proposed in ITA's FY 2018 budget justification has the potential to impact BIS's ability to conduct these checks in a timely manner,[58] requiring BIS to fill any potential coverage gaps so as not to delay licensing or compliance decisions. We plan to review the effectiveness of BIS's enforcement program for end-users to ensure items subject to the EAR are being used in accordance with U.S. policies.

---

[56] *Ibid*, BIS 41.

[57] DOC, *Bureau of Industry and Security, Fiscal Year 2017, President Submission*, BIS 55, and *Bureau of Industry and Security, Fiscal Year 2018, President Submission*, BIS 64.

[58] DOC, *International Trade Administration, Budget Estimates, Fiscal Year 2018*, ITA 47.

Challenge 6: Modernizing the Department's Legacy IT Systems and Improving Data Quality

Although the Department has undertaken numerous initiatives to modernize its IT systems, it continues to rely on antiquated legacy systems to support some of its key functions and processes. For example, 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. In addition, USPTO continues to face challenges in its mission-critical modernization from legacy IT systems to next-generation technology and services.

This challenge focuses on the following areas for management attention:

- Identifying a long-term solution to replace Commerce Business Solutions (CBS)
- Transitioning USPTO from legacy to next-generation IT systems
- Maintaining current, accurate, and complete data to effectively manage real property

Identifying a long-term solution to replace Commerce Business Solutions (CBS)

The Department and most of its operating units use an outdated financial management system (originally implemented more than 20 years ago) that has become increasingly difficult to maintain. 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, reliance on CBS is a continuing high risk for the Department.

The Department plans to replace the CBS legacy financial management system—which does not include features 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 identification of a viable federal shared service provider solution for a replacement. According to the Department, the project is currently on hold as it works with the Office of Management and Budget (OMB) and the Department of the Treasury regarding how to proceed.

As a result, the Department plans to extend use of CBS through FY 2022 by performing critical technology upgrades to keep CBS operational and secure, even though it will be costly and resource intensive. In addition, the Department's challenges also include the uncertainty of adequate funding for timely completion of the replacement project.

Transitioning USPTO from legacy to next-generation IT systems

USPTO operations personnel rely on IT services to examine applications, manage rights, and collect revenue for business operations. However, several major systems are behind their original implementation schedule and over budget. For example, USPTO's Trademark Next Generation system implementation is 5 years behind schedule—and the original estimated

completion costs of $53 million in 2011 have increased to over $200 million (a nearly 300 percent increase). USPTO expects work will continue until at least FY 2019. Additionally, since 2011, USPTO has been developing and modernizing its IT systems used to support patent operations through a new Patent End-to End (PE2E) processing system. While USPTO has made progress, additional improvements are still needed.

USPTO still needs to deploy a number of applications within its IT portfolio and, in the interim, must rely on more than 65 legacy systems to support nearly every aspect of patent and trademark operations. USPTO's goal is to retire the legacy systems as quickly as possible, but the replacement of these IT systems is a multi-year effort and poses a challenge to USPTO's timely deployment of all next-generation IT projects. For example, USPTO's Patent Application Location and Monitoring (PALM) system, used to record and track actions related to patent applications as well as examiner search systems used by examiners for searching patents, were designed in the 1980s for mainframe computers. Until the legacy systems are replaced, USPTO must ensure their stability to meet both internal and external user needs, improve their scalability to support a growing user base and data requirements, provide upgrades, and develop system retirement plans.

USPTO continues to bear the high cost of maintaining a number of legacy systems at the same time that it funds projects that will ultimately replace these systems. For FY 2018, USPTO requested $696.8 million for its IT portfolio, which is a 6.8 percent increase from FY 2017. Of the $696.8 million, 53 percent is associated with maintaining operational activities and 47 percent is associated with project and improvement activities.

Maintaining Current, Accurate, and Complete Data to Effectively Manage Real Property

Management of federal real property has been an area of increased focus for OMB and U.S. Government Accountability Office (GAO) in recent years. OMB memorandums have communicated challenges and required specific actions by all executive branch departments and agencies. GAO has placed federal real property management on its High Risk List since 2003 and has reported on federal real property issues numerous times since.

The Department of Commerce's official database for real property data is the Federal Real Property Management System (FRPM). The Department's Office of Real Property Programs annually inputs FRPM data directly into the Federal Real Property Profile (FRPP) maintained by GSA. Operating units are required to identify underutilized assets in the FRPM. The FRPP also requires the input of facility deficiency estimates under "Repair Needs." NOAA maintains custody of approximately 99 percent of real property owned or leased throughout the Department.

NOAA is required to verify and maintain the accuracy of its data reported in the Federal Real Property Management System (FRPM). In our September 2017 audit report on NOAA's management of real property, we found that NOAA could not substantiate the amounts that were reported in FRPM for all 18 properties reviewed. This occurred because insufficient controls were in place to ensure that (a) the reviewed facilities were adequately documenting

facility deficiencies, and (b) the amounts reported in FRPM were periodically updated as more accurate data became available.

Challenge 7: Implementing Processes to Improve Management of the Department's Contracts, Grants, and Cooperative Agreements

Procurement continues to be a significant support mechanism for the Department's overall mission. The Department's management of contracts, grants, and cooperative agreements has long presented a challenge by virtue of the large amounts of money at stake. In FY 2016, the Department obligated approximately $3.2 billion for goods and services related to satellite acquisitions, support for intellectual property operations, management of coastal and ocean resources, information technology (IT), and construction and facilities management. Additionally, in FY 2016, the Department obligated approximately $1.4 billion in financial assistance awards (grants and cooperative agreements). Appropriate administration of public funds must always be a priority, but, in this climate of constrained budgets, the use of billions of taxpayer dollars requires particular attention from Departmental management.

Key challenges include the following:

- Strengthening processes to govern the appropriate use of non-competitive contracts and maximize the use of competition

- Developing and maintaining a competent acquisition workforce to support the Department's mission

- Improving oversight and monitoring of Minority Business Centers to ensure accurate reporting of program goals and efficient use of program funds

- Fostering high ethical standards throughout the Department and its contracting programs to maintain the public trust

Strengthening processes to govern the appropriate use of non-competitive contracts and maximize the use of competition

In recent years, OMB and the Office of Federal Procurement Policy have focused on improving government acquisition by reducing dollars obligated under high-risk contracts. These include non-competitive contracts and cost-reimbursement contracts. Government-wide guidance called on agencies to maximize the use of full and open competition and to govern the appropriate use and oversight of all contract types to minimize risk and maximize value to the government. Our work has found that the Department continues to face challenges in awarding high-risk contracts without considering the possibility of using less risky contract types.

For example, sole-source contracts are high risk because they are negotiated without the benefit of competition and carry the risk of overspending. Our recent audit of Census Bureau sole-source contracts found that the Bureau lacked internal controls and adequate contracting practices for its sole-source contracts. In our review of 28 sole-source contracts, we found 25 may not fully comply with key pre-award requirements, such as adequate documentation of market research and independent government cost estimates and proper use of statutory authorities. These requirements are essential in helping to ensure that acquisitions are adequately planned, sole-source awards are properly justified, and prices can be demonstrated to be fair and reasonable.

Developing and maintaining a competent acquisition workforce to support the Department's mission

The Department requires a robust and well-qualified acquisition workforce in order to award and administer increasingly complex acquisitions and successfully implement new major initiatives, like category management. In FY 2016, the Department reported that they made progress in the recruitment and retention of a capable workforce that can manage complex acquisition programs. For example, the number of acquisition professionals (GS-1102 series) increased 14.5 percent (from 249 to 285). Also, the attrition rate decreased from 16 to 14.3 percent. Nevertheless, the Department continues to face workforce challenges:

1. The Department's inability to attract and retain experienced acquisition professionals to work in locations outside the Washington, DC, metropolitan area.

2. The Department's inabilities to timely fill vacant positions.

3. The scarcity of talent with the technical expertise and/or program management skills to manage a variety of highly specialized products and services, such as large complex IT systems and scientific and satellite equipment, can be attributed to the fact that the pay scale and incentives in the federal government are not competitive with the private sector.

4. 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.

Improving oversight and monitoring of Minority Business Centers to ensure accurate reporting of program goals and efficient use of program funds

The Minority Business Development Agency (MBDA) faces the challenge of ensuring cooperative agreement funds are administered appropriately and that recipients are accomplishing stated goals. MBDA awards millions of dollars in cooperative agreements annually through its MBDA Business Center program to promote the growth and global competitiveness of minority business enterprises through the mobilization and advancement of public and private sector programs, policy, and research.

While it is important to efficiently award the millions of dollars in cooperative agreement funds annually, it is equally important that MBDA maintains proper oversight over the recipients' use of these funds to ensure accountability and that these funds are effectively used as intended. For example, our audit found that Minority Business Centers (Centers) did not always comply with terms of the financial assistance agreements for collecting and using program income and meeting cost share requirements. Additionally, MBDA should ensure that the Centers are achieving the intended results. However, we found that MBDA did not provide adequate oversight to ensure that these Centers reported reliable data on jobs created and retained and provided required supporting documentation for validating and properly reporting performance accomplishments. Furthermore, MBDA did not consistently document and follow-up on deficiencies found during site visits to Centers, and MBDA did not identify Centers with single audit findings and verify that corrective actions were taken to comply with award terms and

conditions. Without adequate internal controls and oversight, millions of dollars in cooperative agreement funds may not be administered efficiently and effectively, thus raising questions about how effectively these funds are being spent.

Fostering high ethical standards throughout the Department and its contracting programs to maintain the public trust

Our investigations continue to uncover fraud and misconduct related to Commerce contracts and grants. Over the last 4 fiscal years contract and grant fraud allegations accounted for about 26 percent of OIG investigations. OIG efforts in these cases resulted in over $9.9 million in restitution, fines, seizures, and civil settlements for the government, as well as 14 criminal convictions. These cases have disclosed such acts as the diversion of grant funds to convert a lavish ranch into a personal residence for the grant recipient and false billing leading to over $1 million in fraudulent personal gain to the president of a contracting company. Departmental contract and grants personnel are the Department's first line of defense. Increased vigilance can prevent these losses in the first place and also serve to help OIG identify all fraud impeding effective mission accomplishment.

The Department must work harder to foster high ethical standards throughout its federal government contracting programs. In recent years, OIG has repeatedly investigated, and substantiated, claims that the Department's bureaus are improperly awarding lucrative government contracts to former employees or relatives of federal employees without full and open competition. This practice undermines the integrity of government as a whole; fosters a lack of transparency in federal government contracting; and gives the appearance of bias, favoritism, and misuse of official position. In order to maintain the public's confidence that federal officials are acting in the best interest of the U.S. taxpayer, public officials must be more mindful of their actions and adequately document legally sufficient justifications for all actions that may be called into question.

Appendix A: Related OIG Publications

This list presents OIG's FY 2017 work related to top management and performance challenges facing the Department in FY 2018. 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: Census Bureau

- *2020 Census: 2016 Census Test Indicates the Current Life-Cycle Cost Estimate is Incomplete and Underestimates Nonresponse Followup* (OIG-17-020-I; March 16, 2017)

- *2020 Census: Census Bureau Needs to Improve Controls over Administrative Records* (OIG-17-022-A; March 29, 2017)

- *2020 Census: The Address Canvassing Test Revealed Cost and Schedule Risks and May Not Inform Future Planning as Intended* (OIG-17-024-A; May 11, 2017)

- *2020 Census: Evaluation of Interactive Review Address Canvassing Operation Revealed Issues with Quality Assurance Controls* (OIG-17-030-I; September 13, 2017)

Challenge 2: Satellites

- *Audit of the Geostationary Operational Environmental Satellite–R Series: Improvements in Testing, Contract Management, and Transparency Are Needed to Control Costs, Schedule, and Risks* (OIG-17-013-A; February 2, 2017)

Challenge 3: Cybersecurity

- *Inadequate Security Practices, Including Impaired Security of Cloud Services, Undermine USPTO's IT Security Posture* (OIG-17-021-A; March 24, 2017)

Challenge 4: FirstNet

- *Expanding Monitoring Controls Will Strengthen the Management of the State and Local Implementation Grant Program (SLIGP)* (OIG-17-018-A; March14, 2017)

Challenge 5: Trade

- *Enforcement and Compliance Needs to Update and Consistently Implement Its Quality Assurance Policies and Practices* (OIG-17-017-A; February 28, 2017)

Challenge 6: Legacy Systems

- *DATA Act Readiness Review* (OIG-17-015-I; February 17, 2017)

Challenge 7: Grants and Contracts

- *FY 2016 Financial Statements Audit (USPTO)* (OIG-17-002-A; November15, 2016)

- *Audit of Coastal Protection and Restoration Authority Grant Award NA11NMF4630150* (OIG-17-004-A; November 16, 2016)

- *FY 2016 Financial Statements Audit (Department of Commerce) (OIG-17-003-A; November 30, 2016)*

- *National Weather Service's Oversight of Service Contracts, Document Retention, and Reporting Needs Improvement (OIG-17-007-A; November 30, 2016)*

- *Biweekly Reporting on Conference Spending by the Department of Commerce (OIG-17-006-M; December 2, 2016)*

- *NTIA Has Significantly Reduced its Unliquidated Obligation Balances But Can Further Strengthen Review and Documentation Procedures (OIG-17-011-A; December 22, 2016)*

- *2017 Annual Letter to OMB re: Government Charge Card Abuse Prevention Act of 2012 (OIG-17-012-M; January 31, 2017)*

- *NOAA Reviews of Unliquidated Obligations Could Be Improved with Greater Review Frequency and Additional Documentation (OIG-17-014-A; February 3, 2017)*

- *EDA Public Works and Economic Adjustment Assistance Grant Recipient Selections Were Generally Made Competitively But Its Merit-Based Selection Process Can Be Further Improved (OIG-17-019-A; March14, 2017)*

- *EDA Can Strengthen Its Policies and Procedures for Monitoring ULOs (OIG-17-023-A; April 27, 2017)*

- *FY 2016 Compliance with Improper Payment Requirements (OIG-17-025-I; May12, 2017)*

- *Selected Commerce Bureaus Could Improve Review Procedures and Documentation Related to Unliquidated Obligations (OIG-17-026-A; June 12, 2017)*

- *Investigative Report on Alleged Unallowable Costs Under NTIA Broadband Technology Opportunities Program Grant (14-0480; June 15, 2017)*

- *MBDA Can Improve Processes to More Effectively Monitor Cooperative Agreements (OIG-17-029-A; September 5, 2017)*

- *Awarding of U.S. Census Noncompetitive Contracts Did Not Consistently Follow Federal Acquisition Regulations and Commerce Acquisition Policies (OIG-17-031-A; September 25, 2017)*

- *NOAA: Repair Needs Data Not Accurate, and Real Property Utilization Not Monitored Adequately (OIG-17-032-A; September 27, 2017)*

Appendix B: List of Acronyms

ACO	Area Census Offices
AD	antidumping duty
BIS	Bureau of Industry and Security
BPA	blanket purchase agreement
Bureau	U.S. Census Bureau
CBS	Commerce Business Solutions
CEDCaP	Census Enterprise Data Collection and Processing
Centers	Minority Business Centers
CITR	Commerce Information Technology Requirement
CS China	U.S. & Foreign Commercial Service in China
CSP	cloud service provider
CVD	countervailing duty
DOC	Department of Commerce
E&C	Enforcement and Compliance
EAR	Export Administration Regulations
ECMO	Enterprise Cybersecurity Monitoring and Operations
ESOC	Enterprise Security Operations Center
FCC	Federal Communications Commission
FirstNet	First Responder Network Authority
FISMA	Federal Information Security Management Act
FY	fiscal year
GAO	U.S. Government Accountability Office
GM	Global Markets
GOES	Geostationary Operational Environmental Satellites
IAA	interagency agreement
IT	information technology
ITA	International Trade Administration
JPSS	Joint Polar Satellite System
LA-RICS	Los Angeles Regional Interoperable Communications System
LCCE	life-cycle cost estimate
MBDA	Minority Business Development Agency
MHz	megahertz
NASA	National Aeronautics and Space Administration
NESDIS	National Environmental Satellite, Data, and Information Service
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration

NPSBN	Nationwide Public Safety Broadband Network
NRFU	nonresponse followup
NTIA	National Telecommunications and Information Administration
NWS	National Weather Service
OIG	Office of Inspector General
OMB	Office of Management and Budget
OU	operating unit
PALM	Patent Application Location and Monitoring
PE2E	Patent End-to End
PFO	Polar Follow-On
PIN	personal identification number
RAN	Radio Access Network
RMF	Risk Management Framework
SLIGP	State and Local Implementation Grant Program
SP	Special Publication (NIST)
Suomi NPP	Suomi National Polar-orbiting Partnership
the Act	The Middle Class Tax Relief and Job Creation Act of 2012
U.S.	United States
USFCS	U.S. & Foreign Commercial Service
USPTO	U.S. Patent and Trademark Office

11200000294