Testimony of

The Honorable Todd J. Zinser
Inspector General

U.S. Department of Commerce

before a hearing of the

Committee on Appropriations
Subcommittee on Commerce, Justice, Science, and Related Agencies
United States Senate

The Department of Commerce's Fiscal Year 2016 Budget Request

February 26, 2015

Chairman Shelby, Ranking Member Mikulski, and Members of the Subcommittee:

We appreciate the opportunity to testify today as you consider upcoming appropriations for the Department of Commerce. The President's fiscal year (FY) 2016 budget requests $9.8 billion for the Department, not including $3.2 billion for the U.S. Patent and Trademark Office (USPTO). The Department, like other federal agencies, faces significant challenges in the upcoming year. Our October 2014 *Top Management Challenges* (*TMC*) report identifies what we consider to be the most significant management and performance challenges facing the Department of Commerce. My testimony today will summarize several of the concerns and challenges we have identified.

Executive Summary

1. **Enhancing Weather Satellite Development and Mitigating Coverage Gaps:** Technical challenges may increase costs and delay the development and launches of the National Oceanic and Atmospheric Administration's (NOAA's) Joint Polar Satellite System (JPSS) and Geostationary Operational Environmental Satellite-R Series (GOES-R) satellites. For FY 2016, NOAA requested $809 million for JPSS, $380 million for a newly proposed Polar Follow-On, and $872 million for GOES-R.

    *   The first JPSS satellite (JPSS-1) is scheduled for launch no later than the second quarter of FY 2017. Currently JPSS-1 is experiencing an instrument development challenge with the Advance Technology Microwave Sounder (ATMS). To reduce program risks associated with JPSS, NOAA must ensure successful execution of cost, schedule, and performance baselines established August 1, 2013, to keep JPSS-1 on track.

    *   GOES-R is experiencing development challenges that have delayed the launch of its first satellite— currently from October 2015 to March 2016. The revised schedule remains a challenge, and this delay increases the potential amount of time the GOES fleet could be without an on-orbit backup satellite. It is imperative that NOAA and its contractors manage integration and testing schedule progress to avoid repeating previous problems (e.g., a core ground system re-plan of $89 million and a second re-plan—the cost of which has not yet been determined but may cost even more) that could further delay launch.

2. **Addressing Serious Cybersecurity Concerns That Persist:** OIG has identified significant concerns with Department-wide cybersecurity. The Department must address security weaknesses in its incident detection and response capabilities, as well as persistent security deficiencies that make the Department vulnerable to cyber attacks. In addition, vacant positions at the Department's Office of the Chief Information Officer (OCIO) for three senior officials—who are primarily responsible for Department-wide cybersecurity—could further undermine the Department's capability to thwart cyber attacks and complete its enterprise cybersecurity initiatives.

3. **Innovating a Cost-Effective Design for the 2020 Census**: Various program delays have forced the Census Bureau to reevaluate and reduce the timing of 2020 decennial research and testing to meet the September 2015 preliminary design decision for the

2020 Census. The Bureau must also seek ways to overcome several challenges concerning the use of administrative records that would result in a more cost-efficient 2020 decennial. In addition to preparing for the 2020 decennial, the Bureau is conducting its ongoing surveys using a new, realigned field office structure with the goal of reducing the cost of field operations—all while maintaining survey quality and improving response rates. Finally, the Bureau must improve cost accounting practices in order to demonstrate that its decennial programs have achieved actual cost savings.

4. **Providing Stronger Controls Over Finances, Contracts, and Grants:** During the period of FYs 2012–14, the Department obligated over $7.6 billion in contracts and over $3.6 billion in grants. This spending represents nearly one-third of the Department's overall budget during this same period and includes hundreds of millions of dollars in sole source contracts, high-risk contracts and sensitive acquisitions. Our previous audits have noted particular issues with the awarding and monitoring of high-risk contracts, while our annual risk assessments are identifying additional focus areas for future work.

5. **Addressing U.S. Patent and Trademark Office Backlogs, Quality, and Workforce Management:** USPTO's FY 2016 budget request, which includes all of its projected fee revenues, totals $3.2 billion. The agency faces challenges with reducing wait times for issuing determinations on new patent applications, appeals, and other filings—as well as with responding to stakeholder concerns related to patent errors that might lead to abusive and unnecessary litigation. USPTO also faces challenges in managing its large and dispersed workforce.

6. **Addressing First Responder Network Authority (FirstNet) Management Challenges**: FirstNet was established to build, deploy, and operate an interoperable nationwide public safety broadband network (NPSBN). It has been authorized up to $7 billion in funding, to be derived from the proceeds of Federal Communications Commission (FCC) auctions of spectrum licenses, to accomplish its mission. FirstNet's start-up has posed many challenges. Our December 2014 report on ethics- and procurement-related issues found that the Department's monitoring of financial disclosure and potential conflicts of interest at FirstNet was inadequate. We also found that FirstNet contracting practices lacked transparent award competition, sufficient oversight of hiring, adequate monitoring, and procedures to prevent the payment of erroneous and unsupported costs. The Department has acknowledged OIG's findings, concurred with our recommendations, and undertaken corrective actions.

7. **Continuing an Emphasis on Compliance and Ethics:** In FY 2014, OIG investigated and audited several high profile matters—directly resulting from a lack of compliance with laws, rules, regulations and ethics guidelines—that reflected serious mismanagement. Most, if not all, of those matters came to our attention through our hotline. OIG has issued five public reports to be more responsive to our stakeholders, including the Department and Congress, as well as to enhance transparency and accountability relating to programmatic issues or misconduct raised in the complaints. We will continue to devote significant resources to address the matters brought to our attention by whistleblowers. The Department and bureaus have made progress addressing the management issues referred to them through our hotline process, but

further progress requires continued emphasis by OIG and Departmental management.

8. **Ensuring IG Access and Independence**: In August 2014, the Inspector General of the Department of Commerce was one of 47 inspectors general who signed a letter which was sent to Congress concerning access and independence issues occurring at 3 other Departments and agencies. Such issues also occur at the Department of Commerce and vary in degree and form. Several current issues include (1) a 2-year delay from the Department's Office of General Counsel (OGC) in processing audit policies to ensure OIG's unfettered access to records during OIG audits, (2) denied access to "badging-in and -out data" from the Census Bureau headquarters necessary to conduct a data analytics project, and (3) objections to the release of completed reports documenting significant findings and recommendations to Congress or the public; other issues persist. However, OIG was encouraged when—after 8 months during FY 2013, and soon after being appointed—the Secretary resolved the issue created when, in November 2012, NOAA and the Department banned OIG from the monthly Program Management Council meetings for the weather satellite programs.

1. NOAA Must Manage Risks to Keep Next-Generation Satellite Acquisition Programs on Track to Provide Critical Environmental Observations

The Department must actively manage risks associated with the acquisition and development of the next generation of NOAA environmental satellites, as they are its largest investments at more than 20 percent of its $9.8 billion FY 2016 budget request. NOAA requested $809 million for JPSS, $380 million for a newly proposed Polar Follow-On, and $872 million for GOES-R. These satellites are essential components in understanding and predicting the environment: they provide data and imagery used to track severe storms, forecast weather, and study climate and other environmental conditions (see figure 1).

Figure 1: JPSS Program Satellite (Suomi NPP) Captures Blizzard at 1:45 A.M., January 27, 2015
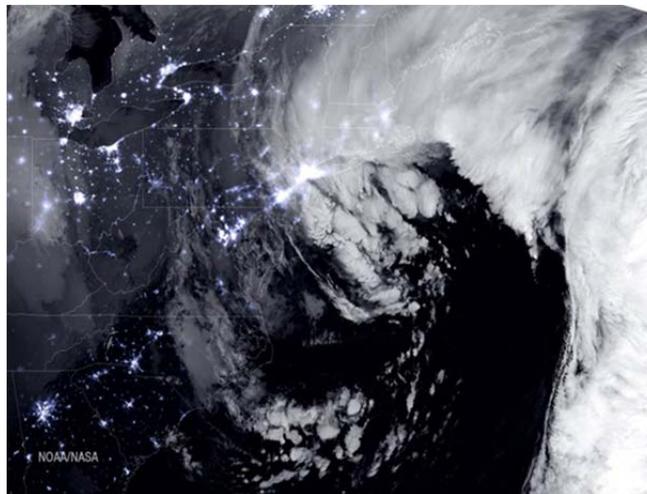
Source: NOAA/NASA via Twitter
(https://twitter.com/NOAASatellites/status/560103060446642178)

The Joint Polar Satellite System (JPSS) program's challenge is to keep the first satellite (JPSS-1) development on track to meet a second quarter FY 2017 launch commitment[1]—while taking steps to implement a newly proposed Polar Follow-On program, which is intended to mitigate a potential data gap in the afternoon polar orbit as well as make the constellation more robust. The Department must also ensure that the Geostationary Operational Environmental Satellite-R Series (GOES-R) program continues to meet requirements and manage development challenges that have already delayed the launch of its first satellite from October 2015 to March 2016, increasing the potential amount of time the GOES fleet could be without an "on-orbit" spare, which is used to back up a failed GOES satellite.

Mitigating Potential JPSS Coverage Gaps

In its FY 2016 budget submission, NOAA requested $809 million for its JPSS program, a decrease of $107 million from the prior year that would not change the program's life-cycle cost of $11.3 billion through FY 2025. NOAA also requested $380 million in FY 2016 for a newly proposed Polar Follow-On system acquisition to reduce potential gaps and extend to FY 2038 operations of its polar satellite system, which includes the procurement of two additional polar satellites (i.e., JPSS-3 and JPSS-4). NOAA plans to manage the Polar Follow-On as part of the JPSS program.

The JPSS program must successfully execute to cost, schedule, and performance baselines established August 1, 2013. The program must also ensure that flight and ground schedules are fully integrated for the JPSS-1 mission. Additionally, NOAA leadership needs to enable the program to effectively manage ongoing development while responding to concerns about the robustness of program development activities (e.g., the need for spare parts for JPSS-1 and -2 instruments and spacecraft), as well as the need for further gap mitigation efforts as proposed in the Polar Follow-On effort. Figure 2 provides a summary of key events.

### Figure 2. Key Events in the Evolution of JPSS Program Baselines (2012–2015)
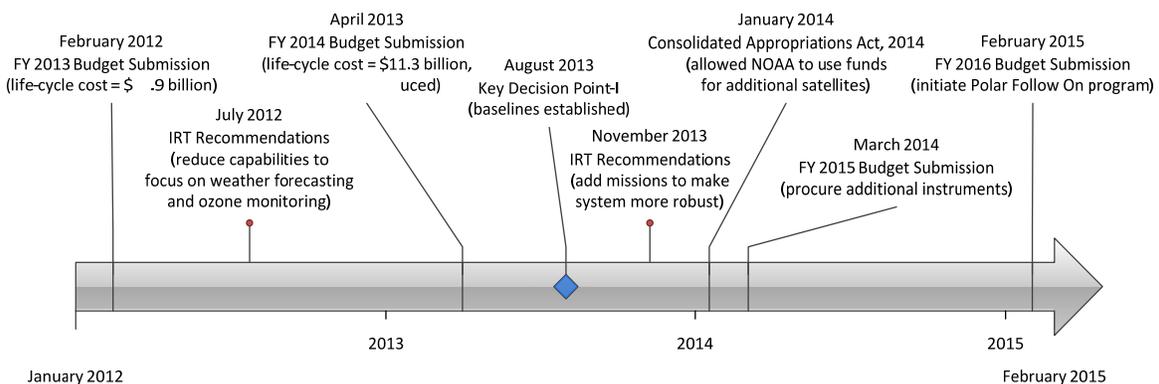
Source: OIG, adapted from NOAA budget, legislation, and JPSS program documentation

---

[1] The program has committed to launch no later than the end of March 2017 but is currently working toward a December 2016 launch.

NOAA's Polar Follow-On system acquisition is in response to an early FY 2014 NOAA independent review team recommendation that the agency adopt a policy to ensure sufficient overlap of missions so that two on-orbit failures would be necessary before a gap in data would occur. The Polar Follow-On proposal in the FY 2016 budget also addresses a recommendation we made in September 2012 that an acquisition strategy for JPSS-3 and JPSS-4 be determined, documented, and shared with the Department, the Office of Management and Budget (OMB), and Congress.[2] Until NOAA implements a viable solution to build robustness into its polar weather satellite constellation, the nation is at risk of a potential gap in critical environmental observations.

In our June 2014 audit report,[3] we continued to raise concerns regarding the time between when Suomi National Polar-orbiting Partnership's (Suomi NPP's) design life ends and JPSS-1 satellite data will become available for operational use. During this potential gap of 10–16 months, there will be significant risk of actual gaps in key data (see figure 3, below). We recommended that NOAA explain the effects of a gap in terms of diminished forecast hours and added economic costs—or, conversely, the contribution to forecast accuracy and the economic benefits of afternoon orbit data.

Figure 3. Potential Gap in Data Continuity Between Suomi NPP and JPSS-1
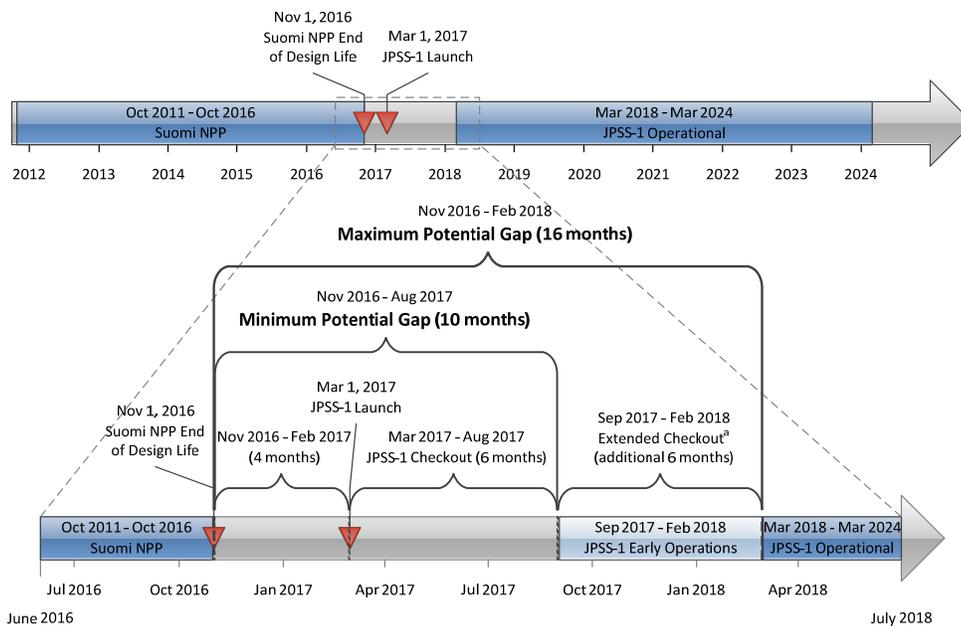
Source: OIG analysis of NOAA data, as of September 2014
[a] Various potential problems could extend the amount of time needed to complete calibration and validation.

---

[2] U.S. Department of Commerce Office of Inspector General, September 27, 2012. *Audit of the Joint Polar Satellite System: Continuing Progress in Establishing Capabilities, Schedules, and Costs Is Needed to Mitigate Data Gaps*, OIG-12-038-A. Washington, DC: DOC OIG.

[3] DOC OIG, June 17, 2014. *Audit of Joint Polar Satellite System: To Further Mitigate Risk of Data Gaps, NOAA Must Consider Additional Missions, Determine a Strategy, and Gain Stakeholder Support*, OIG-14-022-A. Washington, DC: DOC OIG.

Managing GOES-R Program Costs, Schedule Milestones, and System Requirements

The GOES-R program, consisting of four satellite missions (GOES-R, -S, -T, and –U), has an estimated cost of $10.8 billion spread over 37 years.[4] For FY 2016, NOAA has requested $872 million for GOES-R, a decrease of $109 million from the prior year. The program faces acquisition and development challenges that could further delay the launch of its first satellite in FY 2016 or its operational capabilities after launch.

Our ongoing audit assesses the adequacy of GOES-R development activities and NOAA's progress in developing and vetting a comprehensive set of trade-off approaches to mitigate launch delays. Our fieldwork found that late delivery of some flight segment components resulted in NOAA delaying the first GOES-R satellite's launch date from October 2015 to March 2016.

In a March 2014 memorandum,[5] we expressed our initial concerns about NOAA and its contractor. Specifically, multiple problems with ground system development and ineffective communications resulted in two costly re-plans. We observed that, without leadership's attention, the core ground system may not meet minimum requirements for launch in October 2015. Now that NOAA has officially delayed the launch readiness date to March 2016, we believe that the core ground system has a greater likelihood of having all capabilities implemented before launch (see figure 4, next page).

---

[4] FYs 2000–2036.

[5] U.S. Department of Commerce Office of Inspector General, March 6, 2014. *Interim Memorandum re: Audit of NOAA's Geostationary Operational Environmental Satellite-R Series Core Ground System Observations*, OIG-14-014-M. Washington, DC: DOC OIG.

Figure 4. OIG Estimate of the Core Ground System Completion Date,
Based on Progress Made in Implementing Core Ground System Re-Plans
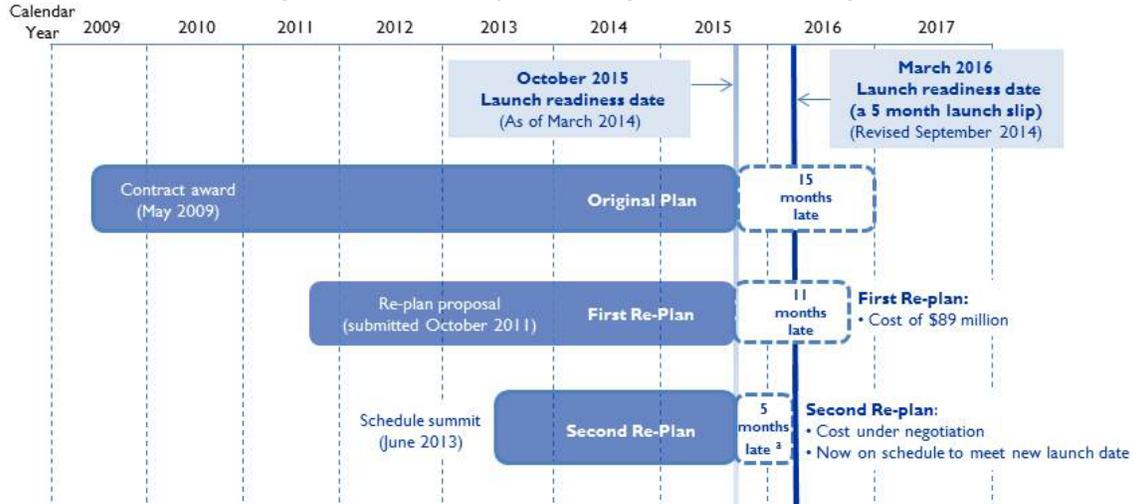
Source: OIG analysis of NOAA data

[a] In March 2014, OIG estimated the core ground system to be 5 months behind schedule based on the launch readiness date of October 2015. OIG's projection of months remaining to develop the core ground system on October 2015 assumed (1) that the contractor would be able to start the second re-plan immediately when it was determined that development was 11 months behind schedule (at the June 2013 schedule summit) and (2) that development time could be re-gained at the same rate as was re-gained by the first re-plan (i.e., 4 months regained over 20 months' duration).

NOAA's integration and test schedule for the first satellite remains a challenge, and the 5-month launch delay has increased the potential amount of time the GOES fleet could be without an on-orbit backup satellite (29 months out of a 33-month period), as shown in figure 5 (next page). If NOAA chooses to reduce capabilities to mitigate an additional launch delay, we would emphasize our 2013 audit report[6] recommendation that NOAA communicate to the National Weather Service and other users—as well as the Administration and Congress—the changes that may be necessary to maintain GOES-R's launch readiness date.

---

[6] DOC OIG, April 25, 2013. *Audit of Geostationary Operational Environmental Satellite-R Series: Comprehensive Mitigation Approaches, Strong Systems Engineering, and Cost Controls Are Needed to Reduce Risks of Coverage Gaps*, OIG-13-024-A. Washington, DC: DOC OIG.

Figure 5. Potential Policy Gaps for GOES Operational Satellites
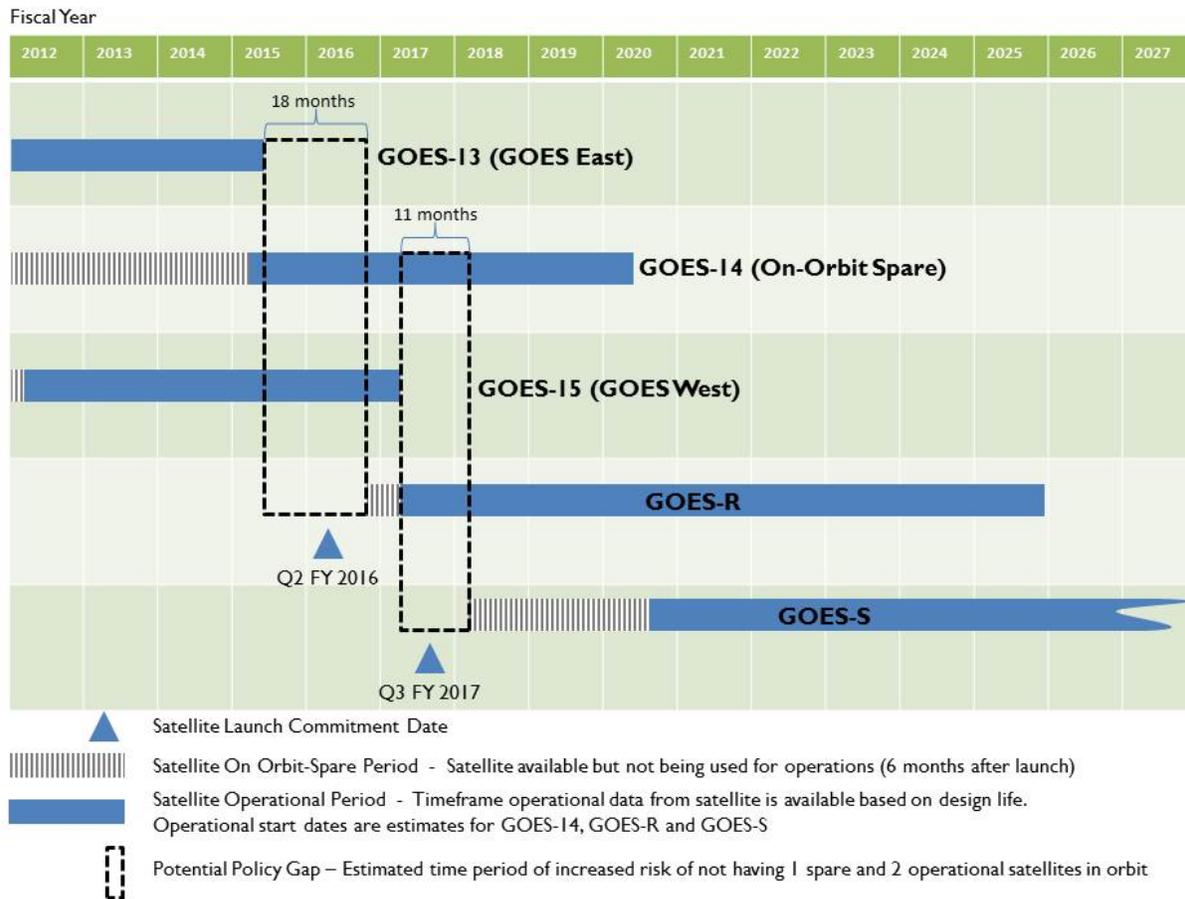
Source: OIG analysis of NOAA information as of December 2014

Ongoing OIG Work

Per House Report 113-448, we have begun a review of the National Environmental Satellite, Data, and Information Service's (NESDIS') common satellite ground system enterprise architecture.[7] Our review objectives are to determine (1) the progress of NOAA's planning efforts and milestones for implementing a common satellite ground system architecture and (2) whether NOAA's plans and efforts provide adequate consideration for system redundancy, security, and scalability. We intend to provide Congress a report by the summer of 2015.

---

[7] Per the report, which accompanied the FY 2015 Consolidated and Further Continuing Appropriations Act (Pub. L. No. 113-235): "The OIG shall provide a report no later than 180 days after enactment of this Act regarding NOAA's existing satellite ground infrastructure and its plans for implementing a common ground system architecture. This report shall include a review of NOAA's planning efforts and milestones for achieving a common ground system and the adequacy of its planning with respect to system redundancy, security, and scalability."

2. Serious Cybersecurity Concerns Persist, and Additional Actions Are Necessary

Although the Department has taken actions to strengthen cybersecurity, our Federal Information Security Management Act of 2002 (FISMA) assessments over the years repeatedly identify significant flaws in basic security measures protecting the Department's IT systems and information. The Department relies on more than 270 IT systems—20 of them categorized as high-impact systems[8]—to support its business operations. Our recent FISMA audits revealed significant security deficiencies in the National Oceanic and Atmospheric Administration's (NOAA's) high-impact systems and identified security weaknesses in the Department's incident detection and response capabilities. Furthermore, in recent OIG *Top Management Challenges* reports, we raised concerns about ongoing Department-wide cybersecurity initiatives to support continuous monitoring. These persistent security deficiencies make the Department vulnerable to cyber-attacks.

Strengthening Cybersecurity Controls

Our recent NOAA IT security audits found that (1) information systems connected to NOAA's critical satellite ground support systems increases the risk of cyber-attacks, (2) inconsistent implementation of mobile device protections increases the likelihood of a malware infection, (3) critical security controls remain unimplemented in its information systems, and (4) improvements are needed to provide assurance that independent security control assessments are sufficiently rigorous. In addition, we identified significant security concerns about NOAA's efforts to reduce the current IT security-related risks within the Joint Polar Satellite System (JPSS) ground system.

In September 2014, NOAA systems were subject to a serious cyber-attack—which caused an interruption of services responsible for providing essential data for weather forecasts and warnings that are vital to the population and the overall economy. This cyber incident highlights the urgency of taking actions to protect critical NOAA systems. We opened an audit as a result (see "Ongoing OIG Work," on page 11, for details on our audit of NOAA IT systems).

Improving Incident Detection and Response

As cyber-attacks continue aggressively targeting IT systems and information, improving the Department's incident detection and response capabilities has become more critical than ever before. We assessed the adequacy of security practices to monitor networks, detect malicious activities, and handle cyber incidents at multiple bureaus—the Bureau of Economic Analysis, Bureau of Industry and Security (BIS), International Trade Administration (ITA), and the U.S. Patent and Trademark Office (USPTO), as well as within the Department's Herbert C. Hoover Building's headquarters—and found that (1) bureaus' actions in response to suspicious network activities may not stop cyber-attacks in a timely manner and (2) a lack of collaboration prevents the bureaus from realizing full benefits of incident detection and response capabilities provided by Managed Trusted Internet Protocol Services, which are part of the Trusted Internet Connections (TIC) initiative.

---

[8] For high-impact systems, a loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on an organization's operations, assets, or individuals.

As a result of the recent successful cyber-attack on NOAA systems, the Secretary directed all Departmental operating units to report cyber incidents to the Computer Security Incident Response Team (DOC CIRT), which will provide required reporting to United States Computer Emergency Readiness Team (US-CERT) and coordination with other outside entities and law enforcement authorities. Previously, only the Department's larger operating units reported cyber incidents directly to US-CERT. However, this process led to lapses in notification to the Secretary's office and to senior management across the Department. For this change in reporting to be effective, the Department must ensure that the DOC CIRT's incident handling capability is sufficiently robust to deal with this additional responsibility. Further, the Department must also ensure that DOC CIRT appropriately notifies OIG and law enforcement of incidents implicating violations of laws.

In addition, in order to improve its overall cybersecurity posture, the Department must maintain a fully operational and stable IT infrastructure at HCHB, which supports core IT services such as incident detection and response to multiple bureaus.

Expediting Department-wide Cybersecurity Initiatives

The Department has several enterprise cybersecurity initiatives under way to address mandates from OMB, including the Enterprise Cybersecurity Monitoring and Operations (ECMO) and Enterprise Security Oversight Center (ESOC) initiatives. ECMO provides nearly real-time security status, support for patch management, and remediation of software configuration issues for Department-wide system components. ESOC—co-located at a NOAA facility in Fairmont, West Virginia—provides Department-wide security situational awareness to senior Departmental and operating unit managers. Ensuring timely implementation of these initiatives is crucial to significant improvement of the Department's cybersecurity posture.

ECMO is an essential piece of the Department-wide continuous monitoring capability. In FY 2016, the proposed funding for ECMO is $3.7 million from the Department's working capital fund (WCF). As of February 2015, all but one of the operating units have deployed the basic ECMO capability on more than 99 percent of their system components; the National Telecommunications and Information Administration (NTIA) lags behind with 70 percent deployed. The Department has made a concerted effort to expedite ECMO deployment and thereby provide nearly real-time security status, support for patch management, and remediation of software configuration issues for Department-wide system components.

In FY 2016, the proposed funding for ESOC is $5.2 million from the Department's WCF. The goal of ESOC is to establish a facility to provide Department-wide security situational awareness to senior Departmental and operating unit managers. While the Department has advanced beyond its ESOC initial planning stage—including completion of ESOC site selection and acquisition of hardware and software for ESOC's operation—it will take several years of the Department's commitment and strong cooperation among operating units to fully implement ESOC capabilities.

Although the Department has made significant progress toward implementing these initiatives, we are concerned that positions within the Department's OCIO for three senior officials primarily responsible for Department-wide cybersecurity have been vacant since

last November. Continuing to leave these positions unfilled could further undermine the Department's capability to thwart cyber-attacks and to complete its enterprise cybersecurity initiatives.

Ongoing OIG Work

Due to the recent cyber-attack on NOAA's IT systems, and given the importance of these systems, we are conducting an audit of NOAA's IT security practices to determine significant factors that contributed to the success of the attack and to evaluate NOAA's handling of the detection, analysis, eradication, and reporting of the attack, as well as recovery from it. Also, as part of our annual FISMA audit work, we are assessing selected IT systems at NOAA, ITA, the Office of the Secretary, and USPTO, as well as IT security continuous monitoring programs at BIS and the Census Bureau. .

3. The Census Bureau Must Design and Implement a Cost-Effective and Accurate 2020 Decennial

Key Statutory Deadlines

March 31, 2017: Deliver Census question topics to Congress

March 31, 2018: Deliver final Census questions to Congress

April 1, 2020: Census Day

December 31, 2020: Deliver state population counts for House apportionment to the President

March 31, 2021: Deliver redistricting data to the states

Source: 13 U.S.C. § 141

The 2020 Census, though 5 years away, is a massive undertaking that requires extensive research, testing, and planning. For 2020, the Census Bureau plans to design and conduct a high-quality decennial operation that costs less per household on an inflation-adjusted basis than Census 2010.

The Census Bureau recognizes that fundamental changes to the design, implementation, and management of the 2020 Census must occur in order to conduct the next decennial at a lower cost than the 2010 Census. The Bureau is currently in the later stage of research and testing and plans to announce a preliminary design decision—which will influence the final decennial costs—in September 2015.

In order to realize its goals, the Census Bureau must improve cost accounting practices in order to demonstrate that its decennial programs have achieved actual cost savings. The Bureau also confronts a number of challenges using administrative records, a key design area related to producing a more cost-efficient decennial for 2020. The challenges include overcoming existing legislative restrictions related to access and data sharing, allaying public concerns about the security of personal data, and ensuring the timeliness and accuracy of the data for decennial census use.

Improving Cost Accounting Practices

Audits of the Census Bureau's 2010 decennial planning noted that the Bureau had not integrated the research and testing schedule with budget and cost data. OIG issued an audit report in May 2014[9] that identified the same issues in 2020 decennial research and planning;

---

[9] 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.

in addition, it concluded that the Bureau's cost accounting practices do not result in actual project cost being recorded in the accounting system. To effectively manage a program of the size, complexity, and cost of the 2020 decennial—and assess the return on investment of research efforts—managers need accurate accounting records. Integration of the research schedule with budget and cost information allows managers to better track the status of available funds, conduct cost-benefit analyses, and forecast impending underruns and overruns so that funds can be reallocated. Without accurate cost information, the Bureau will be challenged to demonstrate in a transparent manner that it achieved cost reduction goals.

In response to our audit, the Bureau is revising its cost-accounting practices. However, the transition to accurate project costing may reveal unexpected cost trends that the Bureau will need to overcome in order to implement innovative design decisions.

Using Administrative Records

A key tenet of the Census Bureau's 2020 decennial redesign efforts is that reducing nonresponse followup operation costs, as well as making other design changes, could reduce the overall 2020 decennial cost by billions of dollars. The use of administrative records[10] to remove nonresponding households from followup operations is critical to reducing these costs. However, the use of administrative records presents challenges: potential legal impediments to data sharing among the Bureau, other agencies, and the private sector exist, as does public sensitivity regarding the use of previously collected data. Consequently, we are concerned that time—to remove legal and other impediments, assess record quality, and successfully incorporate the use of administrative records into the decennial design—may be running out for the Bureau to include this important innovation. Limited or no use of administrative records would hinder one of the key assumptions towards developing new, cost-efficient methods for the 2020 decennial.

Ongoing OIG Work

In monitoring the progress of planning for the 2020 Census, we are currently auditing the 2014 Census Test to evaluate whether test results informed future testing strategies and the extent that research strategies have changed. Since the Census Bureau is committed to conducting the next decennial census at a lower per-household cost (adjusted for inflation) than the previous decennial census, we are assessing the cost estimation practices that the Bureau is currently using to estimate the amount of cost savings that will result from the new design innovations currently in development for the 2020 decennial census. We expect to issue our final report in spring 2015.

In FY 2015 the Census Bureau is conducting four tests: in addition to two site tests there will be two nationwide tests, one on address validation test and another on questionnaire

---

[10] Data collected by federal agencies for program purposes, administrative records contain personally identifiable information that, when combined with other records, can produce statistical information such as demographic, labor force, and socioeconomic indicators. Administrative records have the potential to decrease data collection costs and reduce respondent burden.

content, response options, and languages. The Bureau's two site tests will occur in Maricopa County, Arizona, and the media market area surrounding Savannah, Georgia (which includes Savannah and neighboring counties in South Carolina and Georgia). At the Arizona site, the Bureau will test the effectiveness of computer-based training for the field staff, whether allowing employees to use their own mobile devices to capture census responses is cost-efficient and effective, and how administrative records could fill the gaps in the data collection efforts caused by nonresponding households. (See figure 6, below, showing an enhanced operations control system that will be deployed during the test to allow remote management and oversight of the status and progress of decennial operations.)

Figure 6. Enhanced Operations Control System for Census Bureau Site Test
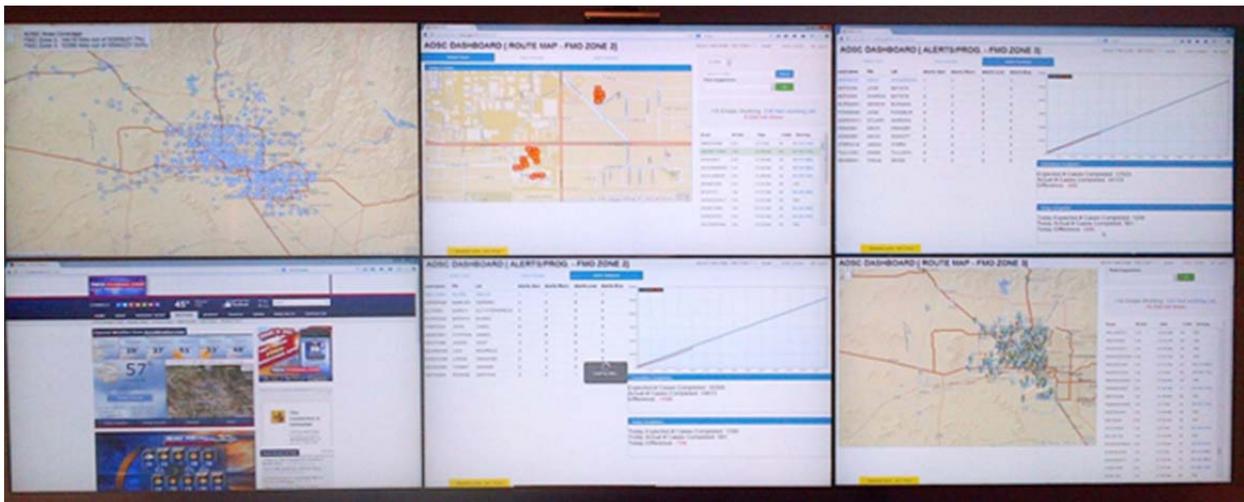
Source: OIG picture of a U.S. Census Bureau simulation exercise

The Savannah test is focused on testing advertising and promotional methods to encourage people to respond online, again with a goal to increase response rate and lower nonresponse followup workload. For example, this test will assess advertising approaches (e.g., the use of targeted social media to reach designated areas, as well as targeted Internet advertising to reach hard-to count areas) and promotion activities (e.g., partnering with local government, business, and nonprofit organizations) to encourage participation.

The 2010 Census costs for conducting address canvassing were $443.6 million. The Census Bureau's nationwide 2015 address validation test will allow the Bureau to assess the performance of the address and map updating methods and models that will shift from a 100 percent address canvassing operation to a targeted address canvassing operation. This test strives to define the address canvassing workloads needed for the operational design decision point in September 2015. The 2015 National Content Test will evaluate and compare different demographic content, contact strategies (including a less costly and more efficient Internet response option) and options for offering non-English materials.

Additional testing activities scheduled in subsequent years will seek to ensure that all procedures and systems are working according to plan prior to the 2020 Census. We will be monitoring the progress of these tests.

We are also planning oversight of the Census Bureau's development of an important IT system that will support its decennial efforts. GAO recently placed the Census Enterprise Data Collection and Processing (CEDCaP) system on its high-risk list. FY 2016 will be the Bureau's second year of the CEDCaP initiative—which aims to integrate and standardize data collection and processing across all surveys (including the decennial census Internet response option), thereby eliminating the single-use, survey-specific systems currently deployed.

4. The Department Must Continue to Strengthen Controls Over Its Finances, Contracts, and Grants

Challenges to the Department's strategic goal of "operational excellence" include controls over budgetary resources, procurement, and overall financial management. Departmental leadership is addressing a number of related issues, including: the management of appropriated funds, the Department's and bureaus' unliquidated obligations, funds spent on conferences, funds spent on premium class travel, modernizing the enterprise financial management system, the Department's working capital fund, and other obligations, including contracts and grants.

Administering High-Risk and Limited Competition Contracts and Managing Post-Award Processes

In FY 2014, the Department obligated about $2.9 billion for goods and services that included satellite acquisitions, intellectual property protection, broadband technology opportunities, management of coastal and ocean resources, IT, and construction and facilities management. Although the Department's spending requirements for goods and services have not diminished, available funding resources likely will remain constrained. For this reason, the Department must institutionalize better and more thorough oversight of its contracts to help management achieve goals, avoid significant overcharges, and prevent wasteful spending.[11]

Table 1. The Department's Non-Fixed-Price Contract Actions,[a] FYs 2012–2014 (in $)

FY	Value of NOAA Contract Actions	Value of Census Bureau Contract Actions	Value of USPTO Contract Actions	Value of All Other Departmental Contract Actions	Total Amount Obligated
2012	616,434,892	68,628,966	195,026,896	40,031,486	920,122,240
2013	595,255,236	53,895,615	197,340,443	50,266,788	896,758,082
2014	629,674,068	94,975,951	351,991,906	72,231,504	1,148,873,429
Total	**1,841,364,196**	**217,500,532**	**744,359,245**	**162,529,778**	**2,965,753,751**

Source: Department of Commerce reporting, www.USAspending.gov
[a] Includes all non-fixed price contract actions.

---

[11] The President has acknowledged contract oversight as a federal government-wide priority; *see* The White House, Office of the Press Secretary, March 4, 2009, "Memorandum for the Heads of Executive Departments and Agencies: Government Contracting."

High-risk contracts. From FY 2012 through February 18, 2015, around 38 percent of the contract obligations awarded by the Department have been high-risk obligations with limited cost restrictions, unlike those associated with fixed price contracts (see table 1, previous page, for data on the Department's non-fixed-price contract actions through FY 2014). Within NOAA alone during this period, more than 70 percent of the contract obligations at the National Ocean Service and more than 60 percent of those within NESDIS are considered high-risk.

In a report issued in November 2013,[12] we reported weaknesses in the awarding and administering of time-and-materials and labor-hours (T&M/LH) contracts at NOAA, NIST, and the Census Bureau. We found that Departmental contracting officers did not award T&M/LH contract actions in accordance with the requirements of the Federal Acquisition Regulation and the *Commerce Acquisition Manual.* T&M/LH contracts are considered high-risk because the contractor's profit is tied to the number of hours worked. We also noted that contract actions in our sample were incorrectly coded in the Federal Procurement Data System (FPDS). In December 2014, we performed this same work at USPTO with similar results.

The Department's challenge is to better monitor and evaluate its T&M/LH contracts through the acquisition and the investment review board processes, which are used to manage the Department's major acquisitions of goods and services. A further challenge it faces is to improve the processes for entering accurate and complete data in FPDS. Effective implementation of the Department's measures will be crucial to ensuring that the Department properly awards, administers, and reports high-risk T&M/LH contracts.

Ongoing OIG work. This year, our work on the Department's high-risk contracts and post-award processes includes audits on:

> *Sole source and limited competition contracts.* From FY 2012 through February 18, 2015, more than 16 percent of the Department's contract obligations were awarded with either no or limited competition, including more than half of those within the National Ocean Service (see table 2, next page, for data on the Department's sole- and limited-source contract actions through FY 2014). As these conditions exist, NOAA is planning to undertake a new approach to contracting for services— Professional and Technical Services (Pro-Tech) Strategic Sourcing Program [13]—that will require significant additional oversight resources.

---

[12] See 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: DOC OIG. T&M/LH contracts are considered high-risk because the contractor's profit is tied to the number of hours worked.

[13] The Professional and Technical Support Services Contract Vehicle, or Pro-Tech, is a strategic sourcing initiative program plan to award contracts which have an estimated value of $3–5 billion over 5 years. The contracts will deliver a wide array of specialty services in the categories of ocean and coastal services, satellite/observing systems services, fisheries, meteorological services, and enterprise operations.

Table 2. The Department's Sole-Source and Limited-Source Contract Actions, [a]
FYs 2012–2014 (in $)

Fiscal Year	NOAA	Census Bureau	USPTO	All Other Bureaus	Total Amount Obligated
2012	248,000,096	66,807,103	55,618,778	81,474,743	451,900,720
2013	165,172,303	45,134,956	50,776,490	81,662,150	342,745,899
2014	194,867,213	56,075,124	68,378,251	80,867,845	400,188,433
Total	608,039,612	168,017,183	174,773,519	244,004,738	1,194,835,052

Source: Department of Commerce reporting, www.USAspending.gov
[a] Includes contract actions not competed, not available for competion or undefined

FAR 6.3 allows for contracting with other than full and open competition under several conditions—including the availability of only one responsible source, an inability for other suppliers or service providers to satisfy agency requirements, or an unusual or compelling urgency. Our future work will consider the risks identified in our various audits and separate analyses to determine how the Department is managing its justifications.

Post-award oversight of fixed price contracts. We are also completing an audit of post-award monitoring and administration of fixed price contracts at NIST. Although our results are still pending, we expect to report additional instances where contracts were not properly administered and contract files were not properly prepared, maintained, or safeguarded for proper security.

Effective contract closeouts. To strengthen oversight of agency acquisition activities, Congress enacted the Services Acquisition Reform Act of 2003, which established chief acquisition officers at all federal agencies except the Department of Defense. The chief acquisition officer is responsible, in part, for monitoring and evaluating the performance of acquisition activities and programs of the Department.

Recent OIG audits and other information have alerted us that the Department is not adequately leveraging contract audit resources or working with the federal government's contract audit experts—the Defense Contract Audit Agency (DCAA)—to identify audit opportunities using a structured approach and risk assessment that takes into consideration Commerce's entire contracting portfolio. We expect to recommend that the Department develop contract administration plans that incorporate contract audits during the pre-award, performance, and post-award phases.

Correctly coding contract actions. Within the last 6 months, we initiated audits at NOAA and NIST to determine whether contracting officials effectively managed and executed undefinitized contract actions.[14] However, because NOAA and NIST

---

[14] Any contract action for which the contract terms, specifications, or price are not agreed upon before performance is begun under the action. Examples are letter contracts, orders under basic ordering agreements, and provisioned item orders, for which the price has not been agreed upon before performance has begun.

incorrectly identified many of its contract actions as undefinitized in FPDS-NG, we had to redirect our efforts toward the reliability of NOAA's and NIST's publicly reported contract information.

Our work is ongoing, but we have continued concerns with the Department's process for entering accurate and reliable data into FPDS and with its controls over the maintenance and safeguarding of contract files. We reported both issues in previous audit reports, and the Department itself has reported similar issues in its Acquisition Management Reviews. Continued errors would suggest that the Department has not remedied outstanding issues over either the reliability of its public data or with missing contract files and documentation. Until the Department better ensures accurate and reliable information is entered into FPDS-NG, it will be of limited use in providing the Congress, Department, and public with a comprehensive view into the details of federal contract spending and increasing the transparency and accountability of the government for how it spends taxpayer dollars.

Monitoring of Obligation Balances

Our June 2013 report[15] on the Department's controls over the management and closeout of obligation balances as of 2011 found inconsistent policies and processes, as well as inadequate monitoring activities. Specifically, we found original obligation balances that could not be verified, accounting records that did not accurately reflect Department obligations, bureaus that did not know the status of its obligations, and improperly liquidated contract obligations.

As a result of our work, we estimated that the amount of unliquidated obligation balances that the Department needed to deobligate was $159 million as of December 31, 2011. The Department did not have adequate internal controls, policies, and procedures to ensure that bureau obligations were adequately monitored and deobligated when appropriate. To address these challenges, the Department's financial management and acquisitions units agreed to five recommendations, including (1) issuing joint final guidance on monitoring open obligations to their respective communities and (2) including routine obligation monitoring as a discussion topic during annual finance and acquisition training sessions. According to the Department's own implementation records, three of our five recommendations have still not been implemented. As a result, we are considering future work on obligations at select bureaus.

Managing the Department's Various WCFs

In its report accompanying OIG's FY 2013 appropriations bill, the Senate Appropriations Committee directed OIG to audit the Department's WCFs. The Department's three WCFs are overseen by the Office of the Secretary, NIST, and the Census Bureau (see table 3, next

---

[15] DOC OIG, June 20, 2013. *Monitoring of Department's Obligation Balances Needs Strengthening*, OIG-13-026-A. Washington, DC: DOC OIG.

page). In May 2014, we issued a report[16] to address Congress' concerns based on issues identified in previous GAO reports.

Table 3. The Department's Working Capital Fund Collections, FYs 2012–2014 ($ amounts in thousands)

Fiscal Year	NIST WCF	Census Bureau WCF	Office of the Secretary WCF
2012	174,245	814,171	153,074
2013	138,620	792,223	145,072
2014	161,249	728,170	165,532
Total	**474,114**	**2,334,564**	**463,678**

Source: Department of Commerce Congressional budget justifications

We reported various issues with the Office of the Secretary's WCF, including the use of incorrect billing rates and inaccurate supporting documentation from service providers for the amounts they charged to customers. As a result, bureau customers were either over- or undercharged for Department services.

Overseeing Premium Travel Spending

In FY 2014, we examined FY 2012 information on the Department's total premium-class travel approved for flight time in excess of 14 hours, as well as for medical disability, which totaled nearly $1.4 million. The difference in cost between premium and coach fares for travel due to flight time in excess of 14 hours was approximately $540,000, while the cost difference due to medical disability was approximately $475,000. With the serious fiscal challenges requiring federal Departments to operate as efficiently as possible, we advised the Department to (1) collect, analyze, and report data on premium-class travel on a periodic basis to the Office of Commerce Services and (2) examine ways to reduce premium travel costs.

> **Ongoing OIG work.** In May 2014, we initiated an audit to evaluate controls over the Department's premium-class travel spending. Specifically, we plan to assess whether the Department has established effective controls over the approval, justification, and documentation of premium-class travel. We will also review the actions taken to implement the recommendations from issues raised in our January 2014 memo.

Other Ongoing OIG Work

> **Managing EDA's revolving loan funds (RLFs).** In May 2014, we initiated an audit of EDA's RLFs. Our audit objective is to determine whether EDA effectively responds to performance problems and changes to distressed communities within the RLF program. While our work is still underway, we are focusing on how EDA may be working with

---

[16] DOC OIG, May 15, 2013. *Office of the Secretary's Working Capital Fund Billing Control Issues Resulted in Incorrect Charges*, OIG-14-020-A. Washington, DC: DOC OIG.

noncompliant RLF and the extent to which those providers expose EDA funds to misuse and economic loss. We are also looking into issues related to capital utilization requirements, high loan default rates, and compliance with reporting requirements.

5. USPTO Must Continue to Reduce Patent Backlogs and Pendency, Address Quality Issues, and Strengthen Workforce Management

In 1990, USPTO became a fully fee-funded organization. For FY 2016, USPTO is requesting authority to spend fee collections of $3.2 billion. In FYs 2013 and 2014, USPTO collected $2.815 and $ 3.172 billion, respectively, in fees. USPTO faces challenges with reducing wait times for issuing determinations on new patent applications, appeals, and other filings—as well as with responding to stakeholder concerns related to patent errors that might lead to abusive and unnecessary litigation. Further—as we testified in November 2014 to the House Oversight and Government Reform and Judiciary Committees—the agency also faces challenges in managing its large and dispersed workforce. Finally, USPTO must make improvements as it undergoes its ambitious IT modernization.

Backlogs and Pendency

Although USPTO has made progress in reducing the time an applicant waits to have a new patent application reviewed (known as "pendency")—as of December 2014, the wait time from initial patent application to an examiner's first action is 18.1 months—waiting times for other types of filings have increased.

The patent application backlog decreased from 718,835 applications in FY 2009 to 610,227 applications as of December 2014, and the pendency dropped from more than 34 months to 27 months during that same time. While the request for continued examination (RCE[17]) backlog decreased from a high of 95,200 in FY 2012 to 44,427 as of December 2014, it still remains far above its low point of 12,489 in FY 2009. The appeal backlog at the end of FY 2014 was 25,506—a slight increase from FY 2013, and still more than twice the backlog level of 12,489 at the end of FY 2009.

Although USPTO has begun to reduce the backlog of RCEs, the rapid rise in the RCE backlog over the last 5 years highlights the challenges USPTO encounters when it prioritizes the review of new applications to the detriment of other types of filings. USPTO must also balance the pressure to issue patents in a more timely manner with its responsibility to ensure that it issues high-quality patents.

Quality Issues

Earlier this month, OIG issued a draft audit report of USPTO's quality assurance programs and will publicly release the report once we have received and address USPTO's comments. Our objectives were to (a) determine the sufficiency of the programs' processes in preventing the issuance of low-quality patents and (b) assess quality reviews performed by USPTO to measure examiner performance.

---

[17] RCEs are patent applications resubmitted for consideration after an examiner has previously closed the review.

OIG's initial findings identify areas for improvement concerning USPTO's quality metrics, its ability to accurately measure patent quality, and management's effectiveness at deterring improper examiner practices. As USPTO explores new options to improve patent quality—such as crowdsourcing searches of relevant technology (or "prior art")—it will, at the same time, need to work to increase stakeholder confidence in its quality assurance processes.

Workforce Management

In our October 2014, report on the *Top Management Challenges facing the Department of Commerce*, we reported that USPTO faces significant workforce management challenges, including operating without a permanent director since January 2013. In the summer of 2014, our office issued two public investigative reports related to concerns with hiring practices at the Trademark Office and waste and mismanagement at the Patent Trial and Appeal Board (PTAB). In the Trademark Office investigation, we found that a senior official intervened in a hiring process to ensure that a non-selected candidate, who was alleged to be the fiancé(e) of a close relative of the official, was ultimately selected for a position as a trademark examiner. In the PTAB investigation, we found that USPTO wasted approximately $5 million in salary and bonuses over a 4-year period on paralegals who had significant idle time and engaged in personal, non-work-related activities while on government time. Although the paralegals billed significant time to a code designated for doing no work, the vast majority of them received the highest performance rating of "outstanding." Moreover, supervisors and senior managers who oversaw the program received over $700,000 in performance bonuses during the relevant time period.

Our October 2014 *Top Management Challenges* report also noted that additional challenges exist with the management of USPTO's telework programs. In response to a hotline whistleblower complaint, USPTO examined allegations of systemic misreporting of time and attendance and how supervisors did not have the tools, and were not empowered by USPTO senior management, to adequately address suspected time and attendance abuse. While these findings and recommendations were not formally issued by the agency, their publication by *The Washington Post* highlighted the need for additional controls and identified challenges that USPTO must address. The Department and USPTO have undertaken a number of initiatives to address these workforce management issues.

Information Technology Modernization

USPTO continues with its Patent End-to-End (PE2E) and Trademark Next Generation (TMNG) acquisition initiatives to significantly improve its IT capabilities to process high quality and timely examination of patent and trademark applications. With USPTO-estimated project costs as of January 2015 of $135.9 million for PE2E and $79.1 million for TMNG, these initiatives represent the most important multiyear IT investments USPTO has undertaken. In evaluating USPTO's management of these acquisitions, we determined that, while progress has been made, improvements can be made to increase software development effectiveness and efficiency. Our review found that USPTO's use of the Agile development methodology for both PE2E and TMNG is maturing. However, we have identified issues and offered recommendations for better managing system requirements,

improving software development testing, addressing IT security earlier in development, and adhering to USPTO's software coding standards.

Ongoing OIG Work

In addition to our ongoing audit of the agency's quality assurance programs, OIG continues its investigation (initiated September 2014) of controls on time and attendance abuse. As part of our FY 2015 audit and evaluation plan, we will also audit Trademark's activity-based information (ABI) system, with objectives to (a) review allocation algorithms and controls of USPTO's ABI system and (b) determine whether Trademark's use of ABI justifies and supports the fees that it charges, as well as any changes to those fees.

6. The Department Faces Key Challenges in Managing FirstNet's Operations as FirstNet Implements a Nationwide Public Safety Broadband Network

FirstNet, an independent authority within the National Telecommunications and Information Administration (NTIA), was established to build, deploy, and operate an interoperable nationwide public safety broadband network (NPSBN) to address the communication failures that occurred during the September 11, 2001, terrorist attacks. The legislation establishing FirstNet provides it with up to $7 billion in funding to be obtained from FCC auctions of spectrum licenses. Prior to receipt of the auction proceeds, up to $2 billion of the amount can be borrowed interest-free from the Department of the Treasury.

FirstNet has indicated that it expended less than $250,000 in FY 2012, around $17 million in FY 2013, and an estimated $27 million in FY 2014.[18] In September 2014, the Board approved a FirstNet budget of $120 million (plus an additional amount to fund remaining FY 2014 authorized obligations) for FY 2015.[19] The FY 2016 budget proposal includes approximately $160 million, at a full-time equivalent level of about 150 positions, to fund FirstNet activities.

FirstNet's start-up has posed many challenges. Initially, it struggled to establish an organization and necessary internal controls. In July 2014, an independent public accounting firm reported a material weakness in FirstNet's financial statements. Additionally, our December 2014 report[20] on ethics- and procurement-related issues found that the Department's monitoring procedures for financial disclosure and potential conflicts of interest at FirstNet were inadequate. We also found that FirstNet contracting practices lacked transparent award competition, sufficient oversight of hiring, adequate monitoring, and procedures to prevent the payment of erroneous and unsupported costs. The Department has acknowledged OIG's findings, concurred with our recommendations, and undertaken corrective actions.

---

[18] Outlays, not expenses, were provided for FY 2012. FirstNet began financial reporting in FY 2013. The FY 2014 results have not been audited yet.

[19] In November 2014, the Finance Committee of the FirstNet Board made available an initial $86 million of the $120 million approved.

[20] DOC OIG, December 5, 2013. *FirstNet Must Strengthen Management of Financial Disclosures and Monitoring of Contracts*, OIG-15-013-A. Washington, DC: DOC OIG.

Subsequently, FirstNet has fallen behind on the schedule it had established for state consultations required by federal law.[21] These consultations are necessary to obtain network cooperation from state and local governments. Finally, FirstNet has encountered difficulties in hiring and maintaining staff for key technical positions.

Organizational Structure

FirstNet has made progress in establishing a management structure. For instance, its Board members no longer play dual roles as Board members and managers. Nonetheless, while many senior positions (e.g., chief information officer, chief administration officer, chief counsel, and chief financial officer) are in place, key leadership positions throughout the organization remain vacant—including the chief user advocacy officer, a leadership position managing consultation and outreach, as well as regional directors and supervisors for consultations. Two FirstNet executives have left their positions, which are now being filled in an acting capacity. To supplement staffing, FirstNet has entered into various interagency agreements and hired contractors. It has also worked closely with the Department in securing important services such as human resources management, ethics compliance, financial management and procurement. Effective oversight of these functions performed on behalf of FirstNet is essential.

Consultation

Cooperation from regions, states, tribes, and localities is a significant factor in ensuring the successful deployment and sustainability of the NPSBN. FirstNet is required by the Act to consult with these jurisdictions regarding the distribution and expenditure of funds required to establish network policies. Accordingly, FirstNet has begun initial consultations with state points of contact and must incorporate the information it collects into the NPSBN's development.

FirstNet had set an internal goal to have initial consultations scheduled by November 2014. However, while FirstNet has held some initial consultation meetings and has scheduled others into September of 2015, many have yet to be scheduled. It is not clear when all initial consultation meetings will be scheduled or completed.

---

[21] The Middle Class Tax Relief and Job Creation Act of 2012 (the Act) authorized the establishment of FirstNet.

Table 4. Status of Initial Consultation Meetings

| Initial State and Local Consultation Status as of February 12, 2015[a]	
Completed	13
Scheduled	18
Not Scheduled	25
Total	**56**

Source: OIG, based on FirstNet data
[a] Deadline for completion: November 30, 2014

Development of a Nationwide Long-Term Evolution (LTE) Network

FirstNet must establish a sustainable NPSBN using $7 billion authorized in the Act, user fees, and agreements with third parties to leverage the value of excess network capacity. Additionally, FirstNet must balance meeting the requests from public safety agencies with developing a network that provides resiliency against environmental and cybersecurity threats. As part of its effort to determine a network design approach, in FY 2013, FirstNet issued a series of requests for information (RFIs) asking for input from vendors and other stakeholders. In FY 2014, FirstNet issued another RFI, to assist in developing a comprehensive network acquisition strategy, and a public notice that seeks input regarding preliminary interpretations of FirstNet's enabling legislation. FirstNet is currently in the process of documenting the response and plans to use the results of the RFIs to help draft the upcoming requests for proposals (RFPs) for the LTE network.

Figure 7. FirstNet's Next Steps Toward Issuing the Draft RFP for the NPSBN
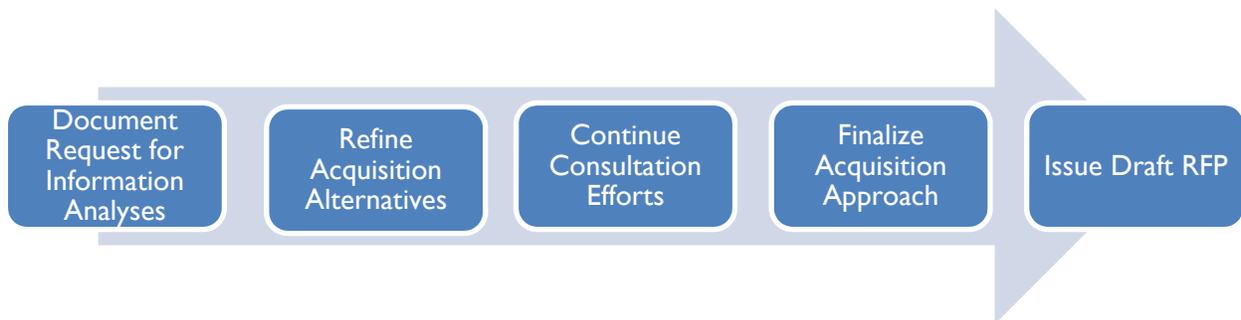

Source: FirstNet

Ongoing OIG Work

OIG continues its oversight of FirstNet. In November 2014, OIG initiated an audit of FirstNet's technical development of the NPSBN. Our objectives will be to evaluate and assess FirstNet's efforts and progress to develop the technical design aspects for the NPSBN against key technical requirements and standards, the requirements of the Act, stakeholder requirements, and established performance metrics and milestones.

7. The Department Must Continue to Foster a Culture of Accountability to Maintain and Strengthen Stakeholder Confidence in the Department.

On April 10, 2014, in written testimony submitted to the Senate Committee on Appropriations, OIG reported that the Department had made significant progress by looking into hotline complaints provided by OIG, reducing the total number pending by half. However, since that time, the number of pending hotline referrals has increased; now there is a risk to the progress made throughout FY 2013 in reducing the backlog and addressing current matters. As of February 13, 2015, there are 76 hotline referrals for which OIG is awaiting an initial management report from bureaus, of which 70 percent are pending with NOAA, USPTO, and the Office of the Secretary. The growing volume of unaddressed referrals demonstrates the need to consistently ensure that issues concerning compliance and ethics are addressed.

Figure 8. Complaint Referrals to Bureaus Awaiting Initial Response
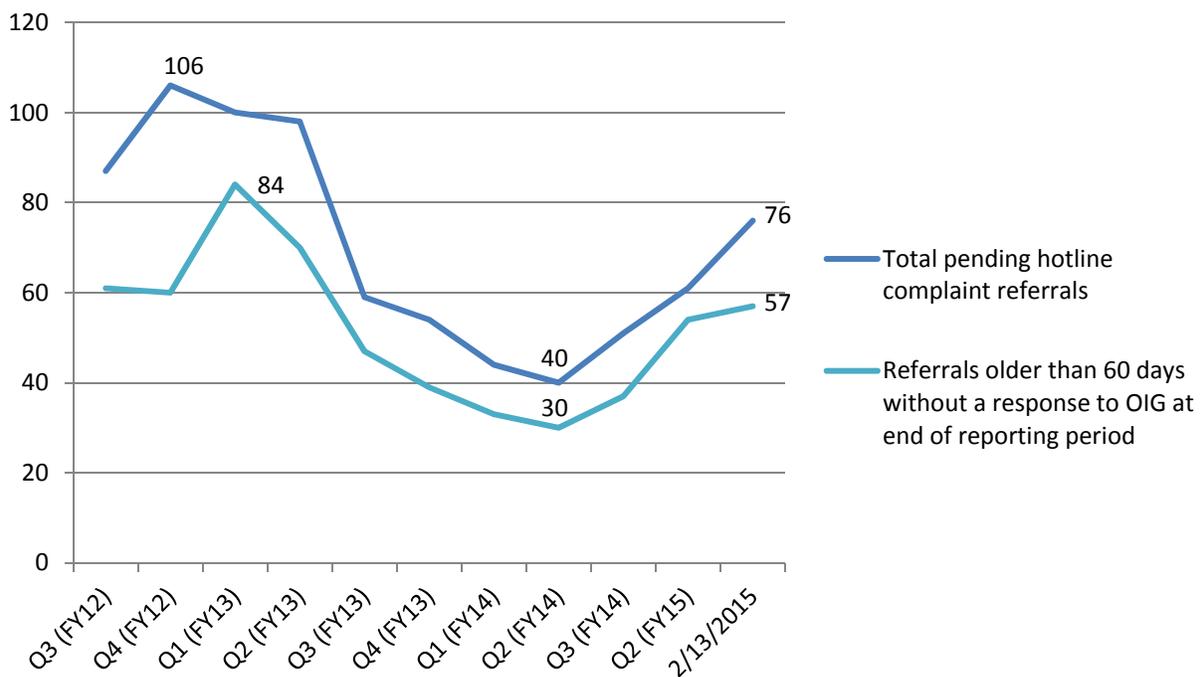
Source: OIG data as of February 2015

While recent management inquiries demonstrate the increased capacity of Departmental officials to look into management matters reported to the OIG hotline and uncover relevant information, three examples of resulting management actions demonstrate mixed results. Two

cases show Department officials taking effective action, and a third illustrates how an agency declined to take disciplinary action where it may have been warranted.

- ***USPTO Proposes Removal After Second Offense:*** In response to an OIG hotline referral in June 2014, USPTO discovered that a patent examiner had advertised on social media being a principal at an IP consulting firm, and that the individual attempted to participate in a patent interview involving a friend. The examiner was informed that participation in the patent interview would present a conflict of interest and—due to the examiner being previously counseled on behavior, communication style, and activity on social media—USPTO issued a proposed removal.

- ***NIST Finds Employees Holding Meetings at Bars:*** In response to an OIG hotline referral, a NIST official found that a manager had held several "meetings" at bars where some employees consumed alcohol while in a duty status. The inquiry official found that one manager received overtime pay for this, and that the manager was engaged in other improper conduct (including making intimidating comments to staff). In light of the inquiry, one manager resigned, and NIST pursued several additional corrective measures.

- ***No Disciplinary Action Taken After Employee Takes Property:*** OIG reported information received over our hotline indicating that recycling materials were being taken from a bureau facility by an employee, which a Bureau fact-finding team confirmed. The inquiry substantiated that the employee (a) derived over $2,000 from recycling materials taken from the government, (b) was dishonest with inquiry officials during an interview, and (c) converted the materials at a recycling center during work hours. Despite implementing controls to attempt to prevent this from happening in the future, the bureau declined to take any action against the employee.

8. The Department Must Ensure that Office of Inspector General Independence and Access is More Strongly Supported

On August 5, 2014, the Inspector General of the Department of Commerce joined 47 other inspectors general in signing a letter to the Chairmen and Ranking Members of the House Committee on Oversight and Government Reform and Senate Homeland Security and Governmental Affairs Committee affirming the importance of access and independence to provide effective oversight. Recently, OIG has experienced several issues concerning Inspector General access and independence:

- ***OIG and GAO Banned from NOAA Satellite Program Management Council Meetings.*** From December 2012 to August 2013, OIG and Government Accountability Office (GAO) auditors were banned from attending monthly Program Management Council (PMC) meetings concerning NOAA's weather satellite programs—meetings that OIG and GAO had historically attended as observers for many years. NOAA's weather satellite programs represent nearly 20 percent of the Department's budget; the PMC meetings include important updates on the progress and decision-making concerning the programs. Despite objections from the Inspector General and two Congressional committees, NOAA refused to permit OIG and GAO attendance. OIG

reported this matter in its April 2013 report[22] concerning its audit of the NOAA's GOES–R Series. The matter was not resolved until the summer of 2013, after the Inspector General raised the issue directly with the Secretary soon after the Secretary's confirmation.

- ***Unreasonable Delays in Processing Audit Policies.*** In order to update the Department's policy concerning OIG's audit processes, OIG is required to have these policies reviewed and approved by the Department's Office of General Counsel (OGC), which has delayed finalizing these policies for 2 years. The policies, which relate to OIG's processes for conducting audits and resolving audit recommendations, respectively, are now being subjected to edits that would explicitly inhibit OIG's independence and access to records needed to conduct audits, evaluations, and inspections. For example, the Department's OGC has proposed the following changes in order to clear, approve, and finalize the policies:

    o Deleting language requiring the Department to provide OIG with direct, full, and unrestricted access to all pertinent records and personnel necessary for conducting audits, inspections or evaluations

    o Deleting language requiring the Department to provide OIG with responsive materials in a timely manner, in the manner requested, and without the use of an intermediary

    o Deleting language stating that the Department shall not impose burdensome administrative requirements to impede OIG access to employees or materials.

    In addition to removing this and other language about cooperating with OIG requests, OGC has requested adding other language inserting its Office into the auditing process; this additional language would direct the OIG to specifically include OGC in the process for obtaining comments on OIG draft reports—even though audit standards require that comments on draft audit reports be obtained from the auditee, not Departmental counsel.

- ***Blocked Access to Badging Data at the Census Bureau.*** In March 2014, following several cases of employee time and attendance abuse at the Census Bureau, OIG attempted to initiate a proactive project to detect potential time and attendance abuse. OIG advised the Bureau of our intent to analyze data generated by employees when they "badge in and out" of the Census Bureau headquarters in Suitland, Maryland. Unfortunately, our attempts to obtain this badging data have been met with substantial resistance. While we have gained access to records for a certain period of time, the Bureau and the Department's OGC have raised legal questions about OIG's access to these records or OIG's use of these records for investigative and disciplinary purposes. We have been provided badging data for a specific population of Bureau employees who are the subject of a specific investigation—but our proactive project to use data

---

[22] DOC OIG, April 25, 2013. *Audit of Geostationary Operational Environmental Satellite-R Series: Comprehensive Mitigation Approaches, Strong Systems Engineering, and Cost Controls Are Needed to Reduce Risks of Coverage Gaps*, OIG-14-024-A. Washington, DC: DOC OIG, pp. 26–27.

analytics to examine a broader universe of badging data has been delayed for nearly a year, while the Department amends its System of Records Notice (SORN), which it claims is necessary to avoid violating the Privacy Act.

- *Senior Official's Threat to Sue the Inspector General for Publicly Releasing an Investigative Report.* In July 2014, the OIG issued an investigative report concerning favoritism, by a senior official at the U.S. Patent and Trademark Office, in the hiring of someone alleged to be the fiancé(e) of a close relative of the official. The senior official was provided the opportunity to review and comment on the report before publication and subsequently threatened to sue the Inspector General under the Privacy Act should the report be made public. This is one of several matters where Departmental officials have asserted that the Inspector General would be violating the Privacy Act by releasing investigative findings to the public, to Congress, or even within the Department. Such assertions, invoking the Privacy Act, raise serious issues of independence and transparency. OIG is currently in the process of amending its System of Records Notice (SORN) to eliminate a current requirement that the public release of investigative findings include consultation with the Department's Chief Privacy Officer—a requirement that essentially provides the Chief Privacy Officer the ability to rule against the public release of OIG reports. OIG will also need Departmental and OMB approval to amend its SORN in this way.

- *Departmental Inaction on Employee Misconduct Investigations.* In February 2014, the Inspector General sent a memorandum to the Acting General Counsel for the Department concerning the lack of action on matters related to employee misconduct. One of the matters included in the Inspector General's memo was a case that had been pending without management action for 18 months after OIG issued a report of investigation to the management. Such inaction undermines accountability and also raises issues of OIG independence; it further underscores the need for OIGs to be able to publicly report cases of misconduct by senior officials without being placed in legal jeopardy under the Privacy Act.

- *NOAA Attempt to Prevent the Release of OIG IT Security Audit Findings by Incorrectly Claiming Findings Were Classified.* In July 2014, OIG released a report on IT security issues concerning four high-impact systems that support NOAA's National Environmental Satellite Data and Information Service. We found numerous significant deficiencies, including the failure to remediate a significant percentage of IT security vulnerabilities identified in two systems by OIG in 2010. Even though NOAA did not raise any objections in its comments to our draft report over a 2-month period, once the final report was issued the agency delayed the public release of the report by asserting it contained national security information and should be classified (i.e., not publicly released). NOAA initiated an investigation of the OIG by the U.S. Air Force, who confirmed that—according to 2007 guidance from the Air Force Space Command—the information contained in OIG's report was not classified. Thereafter, OIG issued its report consistent with its public release practices.

- ***OIG Denied Access to the Results of a Departmental Employee Survey.*** On December 13, 2013, OIG reported serious concerns to the Deputy Secretary about the denial of access to employee survey results. The Department conducted with its employees a "Risk Clarity Survey," which was intended to (a) gauge the extent to which employees were familiar with their obligations to report fraud, waste and abuse; (b) determine whether they were aware of how to report these issues; and (c) solicit any information concerning fraud, waste, and abuse they may have observed. Prior to the survey, the Inspector General was advised that OIG would be provided the survey results. After a more than reasonable period of time, OIG requested the results but the information was not provided. After many months of delay, caused primarily by OGC advising Department officials to not provide OIG with the information, the Inspector General informed the Department that—as a result of the Department's failure to provide the survey results—OIG was required to notify the Secretary and Congress pursuant to Section 5 (d) of the Inspector General Act of 1978 (commonly referred to as a "7-day letter"). Upon the Inspector General informing the Department of OIG's intent, the survey results were promptly provided—notwithstanding guidance from the OGC to the Department advising the contrary.