Top Management and Performance Challenges Facing the Department of Commerce in Fiscal Year 2022

FINAL REPORT NO. OIG-22-001
OCTOBER 14, 2021

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

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

INFORMATION MEMORANDUM FOR SECRETARY RAIMONDO

FROM: Peggy E. Gustafson, Inspector General, (202) 482-4661

DATE: October 14, 2021

CC: Don Graves, Deputy Secretary of Commerce
Zachary Schwartz, Chief of Staff
André Mendes, Chief Information Officer
Wynn Coggins, Acting Chief Financial Officer and Assistant Secretary for Administration
Operating Unit Heads
Operating Unit Audit Liaisons

RE: ***Top Management and Performance Challenges Facing the Department of Commerce in Fiscal Year 2022***
Final Report No. OIG-22-001

The Office of Inspector General (OIG) is required by statute[1] to report annually the most serious management and performance challenges facing the U.S. Department of Commerce (the Department). Attached is our final report on the Department's top management and performance challenges for fiscal year 2022.

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

Challenge 1: Improving the Department's Cybersecurity Resiliency

- Improving the Department's capability to respond to emerging cyber threats
- Maturing the information technology (IT) security program
- Fulfilling the President's executive order on improving the nation's cybersecurity

Challenge 2: Maintaining Continuity, Managing Risks, and Leveraging Investments to Improve Satellite Data, Products, and Services

- Managing technical challenges with polar and geostationary satellites
- Planning and implementing next-generation satellite systems to continue observations and meet future needs

[1] 31 U.S.C. § 3516(d).

- Addressing risks to observations, operations, and communications from frequency interference
- Initiating a space traffic management pilot program
- Leveraging investments for cost-effective weather data, products, and services to protect communities and increase resilience to climate change

Challenge 3: Addressing Departmental Management Matters Involving Acquisitions and Grants

- Ensuring prudent financial management and oversight of pandemic and disaster relief funding
- Improving management and oversight of high dollar/high risk contract portfolios, contract execution, and performance
- Improving the management of IT acquisitions and operations
- Ensuring proper contract and grant file maintenance in virtual and other flexible work environments
- Developing and retaining a competent acquisition workforce to support the Department's mission

Challenge 4: Enhancing Capacity to Enforce Fair and Secure Trade

- Combating unfair trade practices by effectively resolving trade barriers and enforcing U.S. trade agreements
- Protecting national security through effective enforcement of export controls

Challenge 5: Establishing a Strong Framework for Designing the 2030 Census and Improving Operations over Surveys and Employee Background Investigations

- Ensuring data collection is high quality
- Ensuring advertising efforts increase response rates
- Ensuring only candidates suitable for federal government employment are hired

Challenge 6: Meeting Intellectual Property Stakeholder Needs in the Midst of Economic, Technological, and Legal Changes

- Improving efficiency, quality, and timeliness of patent decisions
- Ensuring proper use of the trademark system
- Managing performance of mission-critical services

Challenge 7: Deploying a Nationwide Public Safety Broadband Network

- Ensuring a sound reinvestment process
- Ensuring the successful performance of the contract

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 will be included in the Department's *Annual Financial Report*, as required by law.[2]

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.

[2] *Ibid*.

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: Improving the Department's Cybersecurity Resiliency

In December 2020, cybersecurity company FireEye announced that it had discovered a complex supply chain attack[1] that impacted numerous government organizations and companies around the world.[2] The attack—ultimately attributed to nation-state hackers—led to a series of data breaches.[3] In May 2021, a ransomware attack forced America's largest fuel pipeline to freeze its operations, which greatly affected the East Coast's fuel supply. Later in the same month, another ransomware attack hit the world's largest meat supplier and forced processing plants across the U.S. to halt production. These cyber incidents illustrate the real-life adverse effects cybersecurity vulnerabilities can have on an organization's ability to perform its business functions. As such, they serve as a wake-up call for organizations to take immediate actions to strengthen their cybersecurity posture.

The U.S. Department of Commerce (the Department) faces challenges in strengthening oversight to address longstanding cybersecurity weaknesses. Addressing these weaknesses is key to protecting systems from attacks and other compromises that may pose risks to critical and sensitive data.

The Office of Inspector General's (OIG's) fiscal year (FY) 2022 top management and performance challenges include these priority areas related to cybersecurity:

- Improving the Department's capability to respond to emerging cyber threats
- Maturing the information technology (IT) security program
- Fulfilling the President's executive order on improving the nation's cybersecurity

Improving the Department's capability to respond to emerging cyber threats

Cyber threats and criminals, and their growing sophistication and prevalence, continue to threaten the public and private sectors—and ultimately the American people's security and privacy. According to the Verizon *2021 Data Breach Investigations Report*, public entities are the leading victims of security incidents, behind only the entertainment industry.[4] To counter

[1] A supply chain attack occurs when a cyber threat actor infiltrates a hardware or software vendor's supply chain and employs malicious components or source code to compromise the product before the vendor sends it to their customers. The compromised product then compromises the customer's data or system.

[2] FireEye. *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor* [online]. https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html (accessed July 12, 2021).

[3] The White House. *Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government* [online]. https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/ (accessed July 12, 2021).

[4] Verizon Communications Inc., 2021. *2021 Data Breach Investigations Report*, DBIR. New York, NY: Verizon, pgs. 65 & 84. Available online at https://www.verizon.com/business/resources/reports/dbir/ (accessed July 8, 2021).

increased supply chain threats, and other ever-present threats, the Department needs to ensure effective continuous monitoring and incident response.

Prioritizing the Department's efforts to manage supply chain risk

In December 2020, a major cyberattack was discovered that penetrated both government agencies and private sector companies worldwide, including a Department bureau. The attack, carried out by nation-state hackers through a supply chain attack on SolarWinds, a popular network monitoring software, resulted in a series of data breaches. The incident highlighted the severe impact software supply chain attacks can have and showed an urgent need for the Department to ensure its readiness to combat such threats.

The President's recently signed executive order[5] recognizes the importance of software supply chain security. It directs the Department, through the National Institute of Standards and Technology (NIST), to issue relevant guidelines that include baseline security standards for the development of software sold to the government.[6] Once finalized, the guidelines will be required throughout the federal government. The Department must ensure that it develops these guidelines timely and begins implementing them promptly.

In response to a Congressional request in October 2020, the U.S. Government Accountability Office (GAO) conducted a review of federal agencies' information and communication technology supply chain risk management (SCRM) practices[7] and made specific recommendations to the Department. According to Department officials, progress has been made, but full implementation won't be completed until July 2022. While the Department plays a leading role in developing the federal supply chain security guidelines, it only recently developed a Department-wide SCRM strategy. The Department must ensure it can effectively implement the new strategy to manage its own supply chain risks.

Improving the Department's cyber incident response capabilities and coordination

The Department's ability to coordinate a unified response to cybersecurity incidents is paramount in overcoming increasingly complex and constant cyber threats. While incident response obligations vary among the Department's bureaus, all bureaus are required to coordinate with the Enterprise Security Operations Center (ESOC) when incidents occur. In a

[5] White House, May 12, 2021. *Executive Order on Improving the Nation's Cybersecurity*. Washington, DC: White House. Available online at https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (accessed July 8, 2021).

[6] *Ibid*. *See also* White House. *Fact Sheet: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks* [online]. https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/ (accessed July 8, 2021).

[7] U.S. Government Accountability Office, October 27, 2020. *Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*, GAO-21-164SU. Washington, DC: GAO. Limited official use only.

previous audit,[8] we found that during the Department's investigation into unauthorized access by a former subcontractor, ESOC failed to gain a basic understanding of the affected system and the unauthorized access. This occurred because of a lack of cooperation between ESOC, information system staff, and Office of the Secretary security staff. Additionally, ESOC did not perform a forensically sound examination of the laptops presumably used by foreign national subcontractor employees who accessed and modified a Department system after their contract was terminated. Instead, ESOC's examination contaminated the evidence of potential criminal wrongdoing.

Additionally, in a recent audit,[9] we found that the U.S. Census Bureau (the Census Bureau) missed opportunities to mitigate a critical vulnerability on its remote-access servers before being exploited by an unknown attacker. The Census Bureau remained unaware that its servers had been exploited for 2 weeks because (1) the Census Bureau was not using a security information and event management tool[10] to proactively alert incident responders of suspicious network traffic, (2) the Census Bureau misidentified the direction of malicious network traffic and concluded it had been blocked before entering the Census Bureau's network, and (3) ESOC did not immediately share critical information with the Census Bureau regarding the exploited servers. These delays, caused by both the Census Bureau and ESOC, wasted time during the critical period following the attack, which could have compounded the damage during a more significant cyber incident. The Department must improve its incident response capabilities, procedures, and coordination to be better prepared to respond to incidents affecting its bureaus.

Maturing the IT security program

To effectively minimize cyber threats, the Department must ensure a healthy cybersecurity posture through maturing its IT security program. In our FY 2021 *Top Management and Performance Challenges Facing the Department of Commerce* report (*Top Management Challenges* report),[11] we stated that the Department had not made significant progress in maturing its information security program over the past 2 years, as measured by the *Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*.[12] Our FY 2020

---

[8] U.S. Department of Commerce Office of Inspector General, February 11, 2020. *Failures in the Department's Security Program Resulted in Exposure of Sensitive Trade Information to Unvetted Foreign Nationals*, OIG-20-018-A. Washington, DC: DOC OIG.

[9] DOC OIG, August 16, 2021. *The U.S. Census Bureau's Mishandling of a January 2020 Cybersecurity Incident Demonstrated Opportunities for Improvement*, OIG-21-034-A. Washington, DC: DOC OIG.

[10] A *security information and event management tool* is an "[a]pplication that provides the ability to gather security data from information system components and present that data as actionable information via a single interface." *See* DOC National Institute of Standards and Technology Computer Security Resource Center. *Security information and event management (SIEM) tool (definition)* [online]. https://csrc.nist.gov/glossary/term/security_information_and_event_management_SIEM_tool (accessed July 8, 2021).

[11] DOC OIG, October 15, 2020. *Top Management and Performance Challenges Facing the Department of Commerce in FY 2021*, OIG-21-003. Washington, DC: DOC OIG.

[12] U.S. Department of Homeland Security Cybersecurity & Infrastructure Security Agency, April 17, 2020. *Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 4.0. Washington,

FISMA audit found that the Department again failed to mature its information security program beyond "Level 2: Defined," which was below the federal average of "Level 3: Consistently Implemented." FY 2020 was the third fiscal year in a row where the maturity of the Department's information security program did not improve. Achieving "Level 3: Consistently Implemented" is important because it means the organization has implemented the security controls necessary to protect IT systems and data. Based on our past work and upcoming guidance changes[13] in the cybersecurity landscape, we see significant challenges in FY 2022 as the Department takes steps to mature its program.

Ensuring IT security controls are consistently implemented and effective

In FY 2021, our office initiated an audit to determine the effectiveness of the Department's continuous monitoring and system assessment processes.[14] Ongoing audit work found the Department is not effectively assessing and remediating security controls. Additionally, bureaus are not consistently reporting system assessment results to the Department in the system of record. Therefore, the Department cannot rely on its system of record to reflect accurate system security status for risk-based decisions and allocation of resources at an enterprise level.

Federal agencies are required to continuously monitor and assess system security controls. Periodic system assessments form the basis of the Department's continuous monitoring process by selectively testing system security controls to verify they are consistently implemented and functioning as expected. Without an effective way to monitor security control implementation, it will be difficult for the Department to make meaningful progress in maturing the program to ensure IT security controls are protecting systems as designed.

Managing the security risk of legacy systems

The Department's IT systems and infrastructure are aging and need to be modernized to protect against cybersecurity threats. Keeping systems and their component equipment current is extremely important for security. As noted by the U.S. Department of Homeland Security's Cybersecurity & Infrastructure Security Agency, "[c]ontinued use of EOL [end-of-life] software poses consequential risk to your system[s] that can allow an attacker to exploit security vulnerabilities."[15] In our FY 2021 *Top Management Challenges* report,[16] we noted the Department faced challenges in sustaining modernization priority of legacy systems to strengthen IT security. While the Department works to modernize legacy information systems

DC: CISA, p. 6. Available online at https://www.cisa.gov/sites/default/files/publications/FY_2020_IG_FISMA_Metrics.pdf (accessed July 9, 2021).

[13] In the near future, the Department plans to release its updated IT security baseline policy to incorporate changes reflected in the recently released NIST 800-53 Rev. 5, which supersedes the current NIST 800-53 Rev. 4 standards.

[14] DOC OIG, November 13, 2020. *Audit of the Department of Commerce's System Security Assessment Process*, #2021-389. Washington, DC: DOC OIG.

[15] DHS CISA. *Security Tip (ST04-006). Understanding Patches and Software Updates* [online]. https://www.cisa.gov/tips/st04-006 (accessed July 9, 2021).

[16] OIG-21-003.

and mature its continuous monitoring strategy, several recent audit findings[17] indicate that the Department continues to face significant cyber hygiene challenges related to EOL system components.

Departmental policy requires the bureaus to manage and fund the replacement of EOL hardware and software. In our FY 2020 *Top Management Challenges* report,[18] we identified deficiencies in the United States Patent and Trademark Office's (USPTO's) ability to implement security controls that ensure adequate protection of its legacy systems. In a more recent audit[19] of the Bureau, we found that the Bureau operated public-facing servers that were no longer receiving security updates from the vendor, and the Bureau did not prioritize the decommissioning and replacement of the EOL servers. Lastly, we have observed a similar issue regarding unsupported operating system use in an ongoing audit, initiated November 9, 2020, of the National Oceanic and Atmospheric Administration's (NOAA's) active directory.[20]

Reducing the impact of cyber threats through effective identity and access management

Identity and access management is the process of administering system accounts and privileges so that only authorized users can securely access the specified resources required to perform their jobs. Such accounts act as a gateway to an organization's resources. As a result, this process embodies one of the most critical aspects of an organization's security posture. In April 2021, Colonial Pipeline's IT system was breached through a combination of an inactive user account and the lack of multifactor authentication.[21] This attack led to a disruption in fuel distribution that impacted millions of Americans, which demonstrated the importance of effective identity and access management when facing cyberattacks.

Over the years, we have identified a trend of improper identity and access management, such as excessive privileges of user accounts, weak passwords, and lack of multifactor authentication, within Department bureaus. Our recent audits of the Census Bureau[22] and USPTO[23] found that those bureaus granted users access privileges that were beyond what was necessary for their jobs and did not disable user accounts that were no longer needed. In addition, USPTO did not follow proper password policies as defined in the Department's *Information Technology Security*

[17] *See* (1) DOC OIG, October 16, 2019. *Top Management and Performance Challenges Facing the Department of Commerce*, OIG-20-001. Washington, DC: DOC OIG; and (2) OIG-21-034-A.

[18] OIG-20-001.

[19] OIG-21-034-A.

[20] DOC OIG, November 9, 2020. *Audit of NOAA's Management of Its Active Directory*, #2021-388. Washington, DC: DOC OIG.

[21] CNN. *Ransomware attackers used compromised password to access Colonial Pipeline network* [online]. https://www.cnn.com/2021/06/04/politics/colonial-pipeline-ransomware-attack-password/index.html (accessed July 8, 2021).

[22] DOC OIG, January 7, 2021. *Fundamental Security Safeguards Were Not In Place to Adequately Protect the IT Systems Supporting the 2020 Census*, OIG-21-018-A. Washington, DC: DOC OIG.

[23] DOC OIG, June 13, 2019. *Inadequate Management of Active Directory Puts USPTO's Mission at Significant Cyber Risk*, OIG-19-014-A. Washington, DC: DOC OIG.

Baseline Policy.[24] During our ongoing audit of NOAA's active directory, we have identified similar issues including user accounts having unnecessary privileges, poor password management, and failure to disable inactive accounts.

As evidenced by the attack on Colonial Pipeline, improper identity and access management can increase the attack surface[25] of the Department's IT infrastructure and provides potential attackers with more opportunities to breach the Department's IT systems. In fact, NOAA experienced a significant cyberattack in late 2014 due, in part, to not using multifactor authentication to secure its accounts.[26] Until the Department consistently implements effective identity and access management, this issue will remain a significant challenge to protecting Department IT assets and fulfilling the Department's mission.

Ensuring effective security of the National Public Safety Broadband Network (NPSBN)

The NPSBN is a nationwide wireless broadband network built and customized to meet first responder needs across the United States and its territories. The network is implemented through an arrangement between the federal government and AT&T (NPSBN contractor). While the NPSBN contractor has primary responsibility to build, operate, and maintain the network, the federal government—through the First Responder Network Authority (FirstNet Authority)—retains governance responsibility for the network's safety, security, and resiliency.

Public safety agencies such as the NPSBN are often major targets of nation-states' and cyber criminals' cyberattacks. Effective security of the network is essential to ensure resilient functionality at all times, and especially during times of crisis or emergency.

Oversight of the NPSBN continues to be a challenge for the Department. The FirstNet security scorecard has seen only marginal improvement since a year ago. The Department must provide adequate oversight to ensure the safety, security, and resiliency of the network through effective cybersecurity.

Implementing new security requirements while managing existing challenges

As noted in previous sections, the Department continues to face longstanding challenges implementing and verifying existing security controls. In September 2021, NIST's Special Publication 800-53, Revision 5,[27] became the new standard required by federal law. Dealing with

---

[24] DOC, June 2019. *Department of Commerce Information Technology Security Baseline Policy*, Version 1.0. Washington, DC: DOC.

[25] An *attack surface* is "[t]he set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment." *See* DOC NIST CSRC. *Attack surface (definition)* [online]. https://csrc.nist.gov/glossary/term/attack_surface (accessed July 9, 2021).

[26] 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.

[27] DOC NIST, September 2020. *Security and Privacy Controls for Information Systems and Organizations*, NIST SP 800-53, Revision 5 (updated December 2020). Gaithersburg, MD: NIST. Available online at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (accessed July 8, 2021).

existing challenges combined with the added challenge of transitioning to the new standards and guidelines will collectively be a significant effort.

The differences between the existing Revision 4 and the new Revision 5 are considerable.[28] Major updates include a consolidation of the control catalog; the integration of SCRM and privacy controls; and significant additions to the security control baseline. Revision 5 adds 66 new base controls, 202 new control enhancements, and 131 new parameters to existing controls.[29] Revision 5 also completely renovates control baselines with the addition of new controls and enhancements. With these changes, the system assessment process will play an important role in ensuring adoption. However, the system assessment process is not fully effective, making the transition difficult to manage and monitor.

Fulfilling the President's executive order on improving the nation's cybersecurity

On May 12, 2021, the President signed an executive order on improving the nation's cybersecurity.[30] The order calls for swift, significant action to modernize federal cybersecurity efforts and realign public/private partnership and information sharing within the cybersecurity space.

In addition, the executive order gives the Department a considerable role in establishing future guidelines and practices used throughout both the federal government and the private sector, and calls on the Department to implement significant new security control measures—including agency-wide multifactor authentication and data encryption—by November 2021. The Department must also develop a plan to implement Zero Trust Architecture.[31]

The extensive changes to the Department's technical security controls coupled with prompt deadlines will require considerable effort and resources across the Department and its bureaus. Further, the Department's role, through NIST, will have a significant impact on future federal cybersecurity efforts. Together, these challenges will likely tax an already overburdened IT security program, further magnifying the challenges faced by the Department in its incident response and program maturity efforts.

---

[28] Revision 5 was published in September 2020 and gave agencies a year to prepare for the official withdrawal of Revision 4, which became obsolete on September 23, 2021.

[29] DOC NIST, January 2021. *Analysis of updates between 800-53 Rev. 5 and Rev. 4, by MITRE Corp. for ODNI (xls)*. Gaithersburg, MD: NIST. Available online at https://csrc.nist.gov/CSRC/media/Publications/sp/800-53/rev-5/final/documents/sp800-53r4-to-r5-comparison-workbook.xlsx.

[30] White House, *Executive Order on Improving the Nation's Cybersecurity*.

[31] Zero Trust Architecture is a strategic initiative rooted in the principle of "never trust, always verify" that "helps prevent successful data breaches by eliminating the concept of trust from an organization's network architecture." *What is a Zero Trust Architecture* [online]. https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture (accessed August 10, 2021).

Progress made/challenges remaining since the FY 2021 TMC

During the last fiscal year, the Department and its bureaus made progress in addressing the challenges we identified in the FY 2021 *Top Management Challenges* report[32] by strengthening some aspects of their cybersecurity posture. For example, the Census Bureau and USPTO have implemented all of our prior recommendations for securing the Census Bureau's cloud IT infrastructures and improving USPTO's backup and restoration process.

However, the Department must continuously identify, address, and adapt to evolving challenges affecting its ability to protect its IT systems. The Department must also improve its basic cyber hygiene and monitor for potential threats to prevent unauthorized disclosures that could adversely affect its mission. In addition, the Department continues to face challenges with legacy systems and in consistently implementing and maturing its IT security program. Additionally, securing FirstNet continues to be a challenge. While the Department works to make improvements, we believe it will continue to struggle until the IT security program is consistently implemented across all of the Department's bureaus.

[32] OIG-21-003, pgs. 22–25.

Challenge 2: Maintaining Continuity, Managing Risks, and Leveraging Investments to Improve Satellite Data, Products, and Services

NOAA's environmental satellite systems provide data that are critical inputs to numerical weather prediction models used by the National Weather Service (NWS) and other meteorological organizations to produce weather forecasts and seasonal climate outlooks. Forecasters rely on satellite imagery to track severe storms in near-real time. Other satellite observations include a variety of environmental measurements needed by scientists and emergency managers. NOAA's National Environmental Satellite, Data, and Information Service (NESDIS) is responsible for NOAA's fleet of satellites and environmental data.

NOAA's Geostationary Operational Environmental Satellites (GOES) monitor the Western Hemisphere and provide updates as often as every 30 seconds. GOES imagery and data directly enhance short-term forecasts and inform real-time decisions. NOAA's polar-orbiting satellites—such as the Joint Polar Satellite System (JPSS)—provide atmospheric temperature and moisture profiles that greatly improve the accuracy of 3- to 7-day forecasts. Examples of other satellite observations include sea-surface temperature, space weather phenomena, wildfires, and atmospheric effects on Global Positioning System (GPS) signals that complement polar satellite data.

OIG's FY 2022 top management and performance challenges include these priority areas related to NOAA satellite systems:

- Managing technical challenges with polar and geostationary satellites
- Planning and implementing next-generation satellite systems to continue observations and meet future needs
- Addressing risks to observations, operations, and communications from frequency interference
- Initiating a space traffic management (STM) pilot program
- Leveraging investments for cost-effective weather data, products, and services to protect communities and increase resilience to climate change

Managing technical challenges with polar and geostationary satellites

Completing testing of JPSS-2 and maintaining continuity of polar weather satellite data

NOAA plans to launch the second JPSS satellite (JPSS-2) in September 2022, following a 6-month schedule slip partly related to COVID-19 and other issues.[33] As part of the plan, the JPSS program will conduct environmental testing of JPSS-2 into the 2nd quarter of 2022; this stage of testing can reveal build and workmanship deficiencies that require corrections, potentially further delaying the schedule. Due to the timing for completing environmental

[33] See OIG-21-003, p. 6.

testing, significant technical rework could consume remaining schedule margin, potentially jeopardizing the launch date.

The NOAA-20 and Suomi National Polar-orbiting Partnership (Suomi NPP) satellites fulfill the operational requirement for primary and spare polar satellites, respectively, to ensure data continuity. Suomi NPP has operated for 10 years, which is 5 years beyond its design life. In May 2021, its Cross-track Infrared Sounder (CrIS) instrument had a longwave infrared signal processor failure that caused a loss of capability to provide data for atmospheric temperature and moisture profiles. This data is a key input to computer weather forecasts and is therefore mission critical.[34] In July 2021, NOAA successfully switched to the alternate processor, restoring the longwave infrared data.

The impact of the Suomi NPP CrIS failure was minimal because the NOAA-20 CrIS is fulfilling the primary operational role. However, if the Suomi NPP CrIS alternate processor also fails, its critical longwave infrared capability may be lost, leaving it as a degraded spare. As a result, it is important that NOAA maintain as much of Suomi NPP's capability as possible and carefully manage JPSS-2 technical and schedule risks, including any issues that arise during environmental testing. Both activities are important to avoid failures or delays that could threaten the continuity of NOAA polar satellite observations.

Proving design changes on GOES-T and providing a fully capable geostationary satellite constellation

The next GOES-R series satellite scheduled to launch is GOES-T (which will become GOES-18 on orbit) in February 2022. It will extend the mission lifetime of the operational GOES satellites through 2035. As we discussed in previous reports, GOES-16 and GOES-17 both had performance deficiencies that caused NOAA to delay the GOES-T launch by 18 months, in order to give the GOES-R program time to design, implement, and test changes to address the issues.[35]

The GOES-R program was on schedule after completing comprehensive testing of GOES-T. However, a newly designed propulsion subsystem was installed *after* thermal vacuum testing but *before* mechanical vibration testing. Thus, the subsystem was not in its flight configuration during thermal vacuum testing. Additionally, new Advanced Baseline Imager (ABI) and magnetometer designs will be flying on a GOES-R series satellite for the first time. As a result, potential performance issues are more likely to arise after launch. Performance issues with GOES-16 arcjets and the GOES-17 ABI may potentially shorten their operational lifetimes. NOAA has already announced plans to replace GOES-17 with GOES-T (GOES-18) after it launches and passes initial checks. Therefore, it will be important for the program to prove—after the satellite is on orbit—that its design changes were effective. After GOES-T, there is one remaining satellite planned for the series—i.e., GOES-U.

[34] NOAA indicated that shortwave infrared sounding data could be used in numerical weather prediction model forecasts and, therefore, provide some mitigation for a loss of longwave infrared sounding data.

[35] *See* (1) OIG-21-003, p. 6, and (2) DOC OIG, August 12, 2019. *Geostationary Operational Environmental Satellite–R Series: Program Success Requires Added Attention to Oversight, Risk Management, Requirements, and the Life-Cycle Cost Estimate*, OIG-19-022-A. Washington, DC: DOC OIG.

Planning and implementing next-generation satellite systems to continue observations and meet future needs

NOAA is planning its next generation of satellite systems that will continue key observations and potentially provide new observations that are important to its mission. To do this, NOAA must have sound processes in place to identify and manage its observing requirements. These processes must anticipate and ultimately validate NOAA's needs in the 2030s timeframe.

NOAA previously reviewed its management of requirements and the anticipated user environment that future systems will need to support.[36] It is now planning and formulating follow-on programs in geostationary and low-earth orbits (LEOs, including polar), space weather observations, commercial weather data buys, and ground systems. To support these efforts, NOAA proposed restructuring the NESDIS budget by grouping legacy and new programs under common budget portfolios.[37]

The most mature of its next-generation programs is Geostationary Extended Observations (GeoXO). A review board approved the feasibility of GeoXO's proposed mission and the sufficiency of planning at its mission concept review in June 2021. NOAA requested an increase of $455 million in FY 2022 for GeoXO.[38] A single NOAA program office manages both GOES-R and GeoXO and must now complete GeoXO's concept and technology development phase to refine requirements and prove the proposed system architecture is both responsive to needs and achievable.[39] An important part of this effort will be to validate GeoXO requirements, particularly those beyond the observations of the legacy GOES programs. However, a lack of NOAA-wide distinction among the priorities of observing requirements across line offices has challenged and may continue to challenge the formulation of GeoXO as well as other next-generation programs.

In FY 2022, NOAA plans to initiate the LEO Weather Satellites program, intended both to complement NOAA's current JPSS satellites and serve as a follow-on program. The LEO Weather Satellites program expects to (1) explore the viability of small sounder satellites through an operational demonstration, (2) provide backup to JPSS satellites in the event of an on-orbit failure, and (3) fill an anticipated gap in early morning orbit microwave sounder data. However, these goals will be challenging given typically lengthy satellite system development

[36] DOC National Oceanic and Atmospheric Administration, May 31, 2018. *NOAA Satellite Observing System Architecture (NSOSA) Study*, 2018-05-NSOSA. Washington, DC: DOC NOAA.

[37] Specifically, NESDIS' Procurement, Acquisition, and Construction budget. *See* DOC NOAA, *Budget Estimates Fiscal Year 2022*. Washington, DC: DOC NOAA, NESDIS-5-6.

[38] *Ibid*, NESDIS-101.

[39] NOAA satellite programs follow both NASA and Department frameworks for acquisition program and project management, which align roughly. NASA refers to this as "Phase A: Concept and Technology Development." The Department's corollary phase is "Project Definition" and has similar goals.

timelines, which NOAA intends to shorten with a "smallsat" architecture and "timely innovation using rapid technology infusion."[40]

Addressing risks to observations, operations, and communications from frequency interference

As detailed in our FY 2021 *Top Management Challenges* report, recent and proposed allocations of spectrum for commercial use continue to present risks to NOAA's environmental observations, communications, and operations due to frequency interference.[41]

In late 2020, NOAA performed an assessment that determined spectrum use in frequencies adjacent to a key band used for passive remote sensing by polar weather satellites will interfere with and potentially degrade the quality of those observations and the forecasts that rely on them. These impacts should gradually lessen as the Federal Communications Commission (FCC) implements international limits on out-of-band emissions that will become effective in 2027. Beyond this particular band, NOAA must further study other new commercial uses of spectrum that could interfere with important environmental observations provided by polar satellites.

Additionally, although the FCC authorized a private company to operate in a frequency band adjacent to GPS satellites, it has not yet started operating in this frequency band.[42] As we reported last year, this frequency use will be adjacent to GOES Rebroadcast communications.[43] NOAA and the National Telecommunications and Information Administration (NTIA) are exploring ways that the private company can use the frequency band while minimizing interference.

As was the case in FY 2021, NOAA's challenge is to develop proactive, strategic plans to manage spectrum risk and ensure the success of its missions. To do this, NOAA must have sufficient, knowledgeable staff. NOAA's FY 2022 budget requests an increase of $500,000 and two staff positions to understand and inform decision making on spectrum-related issues.

Initiating an STM pilot program

The Department continues to face challenges in enhancing commercial space technologies and capabilities through the provision of a collision avoidance support service, as envisioned in

[40] DOC NOAA, *Budget Estimates Fiscal Year 2022*, NESDIS-115. NOAA describes its "smallsat" architecture as small satellites, launched into two or three orbits, that it anticipates will be developed and deployed at a faster rate than legacy satellites.

[41] OIG-21-003, p. 8.

[42] As we noted in OIG-21-003, NOAA relies on GPS for many activities, including command and control of its satellites, and it uses radio occultation data of GPS signals as inputs to weather forecast models.

[43] GOES Rebroadcast enables anyone with the proper antenna and software to receive directly full resolution, near real-time GOES data.

Space Policy Directive-3.[44] In 2021, Congress directed NESDIS and its Office of Space Commerce (OSC) to initiate an STM pilot program—in collaboration with industry and federal partners—to (1) develop STM technical prototypes, (2) initiate an open architecture data repository, and (3) perform STM demonstrations and experiments.[45] In addition, Congress approved a merger of OSC and Commercial Remote Sensing Regulatory Affairs (CRSRA), but did not approve a request to transfer these activities out of NOAA.[46]

While OSC/CRSRA funding of $10 million was an increase of $5.9 million in FY 2021, it fell short of the Department's request of $15 million. In FY 2021, OSC lost its politically appointed director and had a staff of five, including an acting director and a detailee. Further, while OSC and CRSRA budgets have merged, those two offices remained distinct in FY 2021 as the new administration determines its whole-of-government approach to STM. While the U.S. Department of Defense (DOD) is no longer required to provide space situational awareness services[47] to non-U.S. government entities after January 1, 2024, it depends on the extent to which the Secretary of Defense determines such actions are necessary to meet U.S. national security interests.[48]

Leveraging investments for cost-effective weather data, products, and services to protect communities and increase resilience to climate change

The Weather Research and Forecasting Innovation Act of 2017 directs investments in affordable advancements in observational, computational, and weather modeling capabilities.[49] With a priority on public safety, it challenges NOAA with improvement in forecasting high-impact weather events and innovation in satellite and data management.

Communities and businesses need reliable data and tools to make informed decisions concerning significant weather events, as NWS aims to protect an increasingly vulnerable American population by providing accurate and actionable products and services.[50] Citing a goal

[44] White House, June 18, 2018. *Presidential Memoranda: Space Policy Directive-3, National Space Traffic Management Policy*, SPD-3. Washington, DC: White House.

[45] U.S. Senate Committee on Appropriations. *Division B-Commerce, Justice, Science, and Related Agencies Appropriations Act, 2021 Joint Explanatory Statement.* Washington, DC: U.S. Senate, p. 41. Available online at https://www.appropriations.senate.gov/imo/media/doc/Division%20B%20-%20CJS%20Statement%20FY21.pdf (accessed July 13, 2021).

[46] *See* (1) Senate Appropriations Committee, *Joint Explanatory Statement*, p. 41; and (2) U.S. House of Representatives Committee on Appropriations. *House Report 116-455 Committee on Appropriations Report for Commerce, Justice, Science, and Related Agencies.* Washington, DC: U.S. House of Representatives, pgs. 45–46. Available online at https://www.congress.gov/116/crpt/hrpt455/CRPT-116hrpt455.pdf (accessed August 17, 2021).

[47] Services that provide knowledge and characterization of space objects and their operational environment to support safe, stable, and sustainable space activities.

[48] 10 U.S.C. § 2274(a)(2).

[49] Pub. L. No. 115-25 (2017), p. 1.

[50] DOC NOAA, *Budget Estimates Fiscal Year 2022*, NOS-1, NWS-1-2.

to invest in climate research, mitigation, and resilience, NOAA's FY 2022 budget requests nearly $7 billion in discretionary authority—a $1.5 billion (28 percent) increase in funding.[51]

Work continues toward many initiatives such as the Weather-Ready Nation, now in its 10th year, designed in part to help decision makers and the public respond to extreme weather, water, and climate events and build community resilience. In addition, NOAA's FY 2022 budget requests $149 million to strengthen core research capabilities, $368 million to improve observing and forecasting systems, and $57 million to make tangible improvements to communities through cutting-edge climate forecasting coupled with a robust approach to diversity, equity, and inclusion.[52] However, maximizing the return on these investments will require a unified approach to research, satellite observations, and forecast services that sustains improvements while maximizing capabilities with cost-effective systems.

Progress made/challenges remaining since the FY 2021 TMC

Our FY 2021 *Top Management Challenges* report discussed aspects of most of these same challenges (with the exception of the "Leveraging investments" section). In FY 2021, NOAA made progress in the following areas:

- The GOES-R program completed design modifications on GOES-T and comprehensive satellite-level testing. Due to delays of unrelated missions scheduled to launch from Kennedy Space Center before GOES-T, NOAA agreed with the launch provider to postpone its planned launch until February 2022.
- The JPSS program completed integration of the instruments with the JPSS-2 spacecraft and is planning to execute satellite-level testing through April 2022 to meet a September 2022 launch.
- NESDIS increased staffing through focused human capital efforts and reduced its expected attrition rates; vacant positions decreased by 70 percent between the 4th quarter of FY 2020 and the 2nd quarter of FY 2021.
- The NESDIS LEO Weather Satellites program began its conceptual phase (or preformulation). The GeoXO program completed its mission concept review in June 2021.
- NOAA submitted its assessment to Congress describing the impact of commercial spectrum use on polar weather satellite observations.
- In addition to receiving Congressional approval to initiate a pilot program, OSC worked with DOD to gain an understanding of DOD's space situational awareness database to inform development of an open architecture data repository.

[51] *Ibid*, NOAA-23.

[52] *Ibid*, NOAA-23–24.

Challenge 3: Addressing Departmental Management Matters Involving Acquisitions and Grants

A continuing challenge for the federal government, and the Department specifically, is spending taxpayer dollars wisely and protecting them from waste and mismanagement. The Department faces ongoing challenges with proper contract and program oversight and performance. In FY 2020, the Department obligated more than $8.6 billion for contractual goods and services related to national environmental satellite service, management of coastal and ocean resources, procurement, acquisition, and construction management, as well as $3.3 billion in grants and other financial assistance awards. As of the 3rd quarter of FY 2021, the Department has obligated more than $1 billion in grant and financial assistance awards in response to the COVID-19 pandemic. OIG audits and evaluations have identified a number of areas where the Department can better manage and oversee contracts to improve program performance; achieve cost savings; and help prevent fraud, waste, and abuse.

The Department must place sustained focus on its contract and grant awards and oversight to ensure these funds are efficiently and effectively spent for their intended purpose and result in the expected quality of services, products, and performance.

OIG's FY 2022 top management and performance challenges for the Department include these priority areas related to acquisitions and grants:

- Ensuring prudent financial management and oversight of pandemic and disaster relief funding
- Improving management and oversight of high dollar/high risk contract portfolios, contract execution, and performance
- Improving the management of IT acquisitions and operations
- Ensuring proper contract and grant file maintenance in virtual and other flexible work environments
- Developing and retaining a competent acquisition workforce to support the Department's mission

Ensuring prudent financial management and oversight of pandemic and disaster relief funding

The Department faces challenges in continuing effective oversight in managing pandemic and emergency relief funds. In 2017 and 2018, the nation experienced historic weather-related disasters—and, in 2020, an unprecedented global pandemic. The Coronavirus Aid, Relief, and Economic Security Act (CARES Act),[53] the Consolidated Appropriations Act, 2021,[54] and the

[53] Pub. L. No. 116-136, 134 Stat. 281 (2020).

[54] Pub. L. No. 116-260 (2020).

American Rescue Plan Act of 2021[55] provided more than $6.9 billion to support the Department's response to the COVID-19 pandemic.[56] A signification portion of the funds allocated went to the U.S. Economic Development Administration (EDA), which received $4.5 billion; NTIA, which received more than $1.5 billion; and NOAA, which received $620 million.

The Bipartisan Budget Act of 2018[57] and the Additional Supplemental Appropriations for Disaster Relief Act, 2019,[58] provided $1.2 billion and $350 million in disaster relief funds to EDA and NOAA Fisheries, respectively, in the wake of separate weather-related disaster events including severe weather, hurricanes, flooding, and wildfires.

In FY 2021, we evaluated EDA's, NOAA Fisheries', and NIST's readiness in implementing and disbursing pandemic relief funds.[59] EDA still faces the challenge of ensuring adequate oversight of financial assistance to impacted communities through grants and revolving fund loans. We previously recommended[60] that EDA develop and implement a comprehensive workforce plan to determine optimal staffing levels needed and identify potential staffing shortfalls or gaps. EDA has taken proactive steps to address this challenge by actively recruiting and hiring talent under the special hiring authority to meet the CARES Act requirements.[61] However, to continue ensuring proper and timely use of the pandemic and emergency relief funds, EDA must ensure that a comprehensive strategic plan is in place and maintain a highly skilled workforce as it increases its oversight of emergency relief assistance appropriations. The significant increase in funding and the need to ensure that these funds are distributed in a prompt and fair manner also come with an increased demand on EDA's workforce, oversight processes, business practices, and financial management systems.

The volume of pandemic funds—and the need to provide assistance quickly while implementing sound controls—poses a considerable oversight challenge in addition to normal grant administration and oversight responsibilities. Our work found[62] that the pace of funds

---

[55] Pub. L. No. 117-2 (2021).

[56] Funds were allocated to the Economic Development Administration, NTIA, NOAA, NIST, and the Minority Business Development Agency to provide assistance to communities affected by and responding to the COVID-19 pandemic.

[57] Pub. L. No. 115-123, 132 Stat. 64 (2018).

[58] Pub. L. No. 116-20, 133 Stat. 871 (2019).

[59] *See* (1) DOC OIG, January 5, 2021. *EDA Was Effective in Implementing the Requirements for Awarding Funds Under the CARES Act*, OIG-21-017-I. Washington, DC: DOC OIG; (2) DOC OIG, June, 9, 2021. *NOAA Fisheries Implemented the Requirements for Awarding Funds Under the CARES Act but Faces Challenges with the Pace of Funds Disbursement to Fishery Participants*, OIG-21-028-I. Washington, DC: DOC OIG; and (3) DOC OIG, August 5, 2021. *NIST Was Effective in Implementing the Requirements for Awarding Funds Under the CARES Act*, OIG-21-032-I. Washington, DC: DOC OIG.

[60] DOC OIG, January 27, 2020. *EDA Should Develop a Workforce Plan and Improve its Hiring Accountability to Successfully Award and Administer the Disaster Supplemental Funds Appropriated by the Bipartisan Budget Act of 2018*, OIG-20-014-A. Washington, DC: DOC OIG.

[61] Economic Development Administration. *CARES Act Talent Management Database* [online]. https://eda.gov/careers/opportunities/cares-act/index.htm (accessed June 23, 2021).

[62] OIG-21-028-I.

disbursement to NOAA Fishery participants was not consistent with the Office of Management and Budget's (OMB's) guidance,[63] which emphasizes the importance of agencies distributing CARES Act funds in an expedited manner. GAO also found that NOAA was inconsistent in distributing the CARES Act funds in an expedient manner as outlined in OMB's guidance.[64] To address the issue, NOAA began requesting periodic reports from grantees in order to track the progress of the disbursement of funds by the states, Tribes, and territories and developed a method to track funds disbursement.

The need to disburse funds quickly can hinder the effectiveness of existing controls and create additional opportunities for individuals to engage in fraud. It is imperative that Department bureaus put in place controls to safeguard taxpayer dollars and prevent improper payments. Failing to heed the lessons learned in the implementation and disbursement of pandemic relief funds will result in increased fraud and more dollars diverted from those awaiting economic relief.

Improving management and oversight of high dollar/high risk contract portfolios, contract execution, and performance

Our work continues to identify challenges and opportunities to improve the Department's oversight of contracts in order to put taxpayer dollars to better use. Several programs rely heavily on external contractor support to provide a wide array of complex services such as human resource management and administration, ship planning and execution activities, and enterprise software development and implementation:

- In 2016, the Department entered into a Blanket Purchase Agreement (BPA) with a cumulative value of $550 million to provide human resources and program management support and other consulting services to bureaus within the Department. Our previous and ongoing work[65] indicates that Enterprise Services (ES) faces significant challenges in contract oversight and performance management.
- The NOAA ship and aircraft recapitalizations are complex, multi-year acquisitions that require effective planning, execution, and oversight to ensure that the ships and aircraft provide maximum long-term benefit to the Office of Marine and Aviation Operations (OMAO) and the taxpayer. Prior work[66] pertaining to NOAA's ship recapitalization has

[63] Office of Management and Budget, April 10, 2020. *Implementation Guidance for Supplemental Funding Provided in Response to the Coronavirus Disease 2019 (COVID-19)*, M-20-21. Washington, DC: OMB. Available online at https://www.whitehouse.gov/wp-content/uploads/2020/04/Implementation-Guidance-for-Supplemental-Funding-Provided-in-Response.pdf (accessed July 20, 2021).

[64] GAO, January 2021. *COVID-19: Critical Vaccine Distribution, Supply Chain, Program Integrity, and Other Challenges Require Focused Federal Attention*, GAO-21-265. Washington, DC: GAO.

[65] See (1) DOC OIG, September 24, 2020. *Management Alert: Enterprise Services Did Not Perform Adequate Contract Oversight to Prevent Delays and Errors in Processing of Employees' Pay, PARs, and Benefits*, OIG-20-051-M. Washington, DC: DOC OIG; and (2) DOC OIG, February 11, 2020. *Audit of Enterprise Services Performance in Managing and Overseeing Accenture Blanket Purchase Agreement No. DOCSS130116BU0004 and Subsequent Call Orders*, #2020-363. Washington, DC: DOC OIG.

[66] See (1) DOC OIG, November 12, 2019. *NOAA's Office of Marine and Aviation Operations Needs to Improve the Planning and Governing of Its Ship Fleet Recapitalization Effort*, OIG-20-006-A. Washington, DC: DOC OIG; and

identified several acquisition areas NOAA needs to improve upon, such as acquisition planning governance, requirements management, funds oversight, and costs and schedule management.

Effective acquisition planning, execution, management, and monitoring will help ensure that these programs are implemented on time and operate effectively and within cost estimates. Further, proper oversight will help ensure that contractors are held accountable for performing the work required in accordance with specifications. The Department needs to develop and implement procedures and controls that ensure that contract cost, schedule, and performance are adequately monitored and contractual requirements are enforced to mitigate risks and ensure the success of the programs.

Improving the management of IT acquisitions and operations

GAO[67] lists IT acquisitions and operations as a high-risk area and has reported that these investments often suffer from a lack of disciplined and effective management in the areas of project planning, requirements definition, and program oversight and governance.

Beginning implementation of the Business Applications Solutions (BAS) program

As a top IT modernization priority of the Department, the BAS program seeks to deploy (1) an integrated suite of financial management, acquisitions management, and property management applications; (2) an enterprise data warehouse; (3) business intelligence reporting; and (4) data archiving solutions in a hosted environment. In 2020, the Department awarded a firm fixed-price contract for the BAS program and related services worth about $341 million through FY 2040. Through this contract, the Department will acquire licensing and hosting services for the BAS system's three new software applications. In April 2021, we observed[68] that (1) the BAS program lacked plans for business process reengineering and (2) ongoing process change efforts were not consistent with best practices.

The BAS program plans to begin its first of three phases of implementing the new system at NOAA during FY 2022.[69] While conducting this and other implementation phases, the program must overcome challenges such as significant business process reengineering and organizational change management efforts as it consolidates business functions currently supported by disparate legacy systems. The program must manage requirements, develop a business process

(2) DOC OIG, May 25, 2021. *OMAO Must Define and Implement a Disciplined Requirements Management Process to Ensure Future Acquisitions Meet User Needs*, OIG-21-027-I. Washington, DC: DOC OIG. *Note:* Our office contracted with the MITRE Corporation—an independent firm—to perform this evaluation.

[67] GAO, March 2, 2021. *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, GAO-21-119SP. Washington, DC: GAO.

[68] DOC OIG, April 19, 2021. *Management Alert: BAS Program's Focus on Technology May Overlook Risks Related to Business Processes*, OIG-21-023-M. Washington, DC: DOC OIG.

[69] The BAS program plans to implement acquisition and financial management applications for NOAA in FY 2022 and update the property management application, which the program launched across the Department in April 2021.

reengineering plan, capture adequate risk information, optimize processes independent of technology, and implement the new system using a consistently applied methodology.

Preparing for the transition to a common grants management system

The Department intends to replace three different grants management systems used by the bureaus with a common Grants Enterprise Management System (GEMS). The GEMS program is expected to reduce costs and complexity and standardize grants data across the Department.

After an analysis of alternatives, the Department chose the National Institutes of Health's (NIH's) Electronic Research Administration (eRA) systems as the solution for GEMS. NIH will provide operations and maintenance support through FY 2026. By the end of FY 2022, the GEMS program plans to transition EDA and NOAA to eRA, along with bureaus that NOAA currently serves with its legacy grants system. GEMS will transition NIST and NTIA to the new system by the end of FY 2023; NIH will provide operations and maintenance support through the 2nd quarter of FY 2026.

The budget for the GEMS program from FY 2019 to FY 2023 is $26.8 million. The Department needs to monitor GEMS costs, schedule, and performance as well as risks to ensure program success. Given the need to disburse funds expediently and conduct effective oversight of grants programs, the GEMS program must manage the migration of data from legacy systems and transition bureaus to the new system without interruptions or data loss.

Ensuring proper contract and grant file maintenance in virtual and other flexible work environments

OMB directed agencies to utilize technology to the greatest extent practicable to support mission continuity during the COVID-19 pandemic.[70] Beginning in March 2020, the Department required all telework-eligible employees to move to full telework until further notice. Department employees have continued to work remotely until protocols are in place for safely returning to the office. Due to the telework requirement, the Department must now electronically administer and manage contract and grant files for multiple contractors and grantees in a virtual environment.

Our prior audit work[71] has repeatedly identified significant vulnerabilities in the management of contract and grant file documentation that could expose the Department to substantial financial losses. With the Department's increase in funding due to the pandemic and employees working remotely, the Department's efforts to manage and retain contract and grant files can present additional management challenges. In many cases, the Department's bureaus physically maintain contract and grant files at their office locations. There is a lack of Departmental guidance on how contract and grant files and any other required documents should be maintained and

[70] OMB, March 22, 2020. *Harnessing Technology to Support Mission Continuity*, M-20-19. Washington, DC: OMB.

[71] *See* (1) DOC OIG, June 2, 2020. *The Department Needs to Improve Oversight Practices to Close Out Contract Files by Complying with Federal Regulations and Departmental Requirements*, OIG-20-028-A. Washington, DC: DOC OIG; and (2) DOC OIG, August 12, 2019. *Audit of NOAA Financial Assistance Awards to the Gulf States Marine Fisheries Commission*, OIG-19-021-A. Washington, DC: DOC OIG.

stored in an all-virtual environment. This may lead to poor file maintenance and increase the likelihood of improper payments, insufficient support for contract actions, and issues with the contract closeout process. Furthermore, any failure to adequately maintain contract and grant files creates significant financial risk and demonstrates a lack of internal control over the Department's contract and grant actions.

The Department needs to ensure its contract and grant functions are equipped to respond to virtual and other flexible environments in order to accommodate multiple remote work sites.

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

The Department's ability to hire and retain experienced acquisition staff is an ongoing challenge. The services provided require well-qualified acquisition personnel to award and administer progressively more complex acquisitions and successfully set a priority of workload distribution that aligns with the Department's strategic goals. The federal acquisition workforce requires the technical expertise and program management skills to manage a variety of highly specialized products and services, such as large, complex IT systems and scientific and satellite equipment. In FY 2020, the Department saw an 8 percent increase (from 307 to 331) in the number of acquisition professionals in the GS-1102 (Contracting) job series. In addition, the attrition rate decreased by approximately 6 percent (from 53 to 34).

During FY 2020, the Department has continued to address this issue of managing and strengthening its acquisition workforce. In collaboration with the Office of Human Resources Management, the Department has made progress in its recruitment efforts to maximize incentives and devise strategies to recruit and retain entry- and mid-level acquisition personnel. The Department enhanced its recruitment and retention efforts related to (1) building a pool of mid-level professionals, (2) using the Pathways Programs, and (3) using special hiring authorities. These efforts have been aimed at attracting and retaining highly qualified employees to meet hiring projections for a staff of 337 acquisition professionals. Although its aggressive recruitment effort resulted in filling 31 positions, the Department fell short of its staffing goal. In addition, the Department continues to face the following critical workforce challenges that we have noted in prior *Top Management Challenges* reports:[72]

- difficulty in attracting and retaining experienced acquisition professionals to work in locations outside the Washington, DC, metropolitan area
- timeliness of filling vacancies
- shortage of talent due to federal government pay and an incentives package that is not competitive with the private sector
- other factors including budget cuts, a legislative hiring cap, lack of relocation funding incentives, and limited career development and advancement opportunities

[72] See OIG-21-003 and OIG-20-001.

Progress made/challenges remaining since the FY 2021 TMC

The Department and its bureaus have made some progress on our previously reported FY 2021 top management and performance challenges, as noted below:

- During FY 2021 we found that EDA, NOAA Fisheries, and NIST were effective in implementing the requirements for awarding funds under the CARES Act.[73]
- The BAS program launched its property management software, Sunflower, in April 2021, and by October 2021 will have concluded its design phases (global design and common solution).

The Department, however, continues to face challenges in several areas that we had previously identified:

- In FY 2021, we reported that NOAA and OMAO did not have current long-range strategies and processes for managing fleet requirements—which, in turn, could impact OMAO's ability to efficiently respond to and evaluate changing conditions.[74] NOAA should continue to take steps to improve requirements management, planning, and oversight of its ship recapitalization efforts.
- ES is responsible for effective administration and oversight of the BPA and subsequent call orders providing human resources and program management support and other consulting services to bureaus within the Department. We previously reported[75] in FY 2020 that the vendor did not resolve delays and errors in processing employees' pay, personnel action requests, and benefits in a timely manner. ES continues to be challenged with providing effective contract monitoring and oversight. Our ongoing work[76] indicates that ES did not adequately assess contractor performance and that contracting officials did not properly monitor funds, review invoices, or ensure that the contractor performed work prior to approving invoices for payment. Inadequate oversight and monitoring increase the risks of improper payments; payment for work not performed; and fraud, waste, and abuse. The Department needs to develop and implement procedures and controls that ensure that contractual performance is adequately monitored and contractual requirements are enforced.

[73] *See* (1) OIG-21-017-I, (2) OIG-21-028-I, and (3) OIG-21-032-I.

[74] OIG-21-027-I.

[75] OIG-20-051-M.

[76] DOC OIG, #2020-363.

Challenge 4: Enhancing Capacity to Enforce Fair and Secure Trade

As one of the federal government's leading trade enforcement and promotion agencies, the Department faces the continuing challenge of helping U.S. companies be more competitive abroad and attract foreign investment while protecting U.S. national security interests. These responsibilities primarily reside with two Departmental bureaus:

(1) the International Trade Administration (ITA), which assists U.S. exporters with selling their products overseas and enforces U.S. trade laws and agreements, and

(2) the Bureau of Industry and Security (BIS), which administers and enforces U.S. export control laws and regulations.

The President's *2021 Trade Policy Agenda*[77] prioritizes opening foreign markets and reducing trade barriers. Additionally, the Administration's trade policy aims to increase economic security for American families through combating unfair practices by U.S. trading partners. Among its trade priorities are (1) protecting U.S. businesses from the People's Republic of China's (China's) unfair and coercive trade practices—including nontariff barriers to restrict market access, unfair subsidies, and illicit acquisition of technology—and (2) enforcing U.S. trade agreements with foreign trade partners.

OIG's FY 2022 top management and performance challenges include these priority areas related to trade enforcement:

- Combating unfair trade practices by effectively resolving trade barriers and enforcing U.S. trade agreements
- Protecting national security through effective enforcement of export controls

Combating unfair trade practices by effectively resolving trade barriers and enforcing U.S. trade agreements

The Secretary of Commerce has stated that the Department is committed to holding U.S. trading partners accountable when they violate U.S. laws and trade agreements. The Secretary's focus is proactively identifying, monitoring, and resolving trade barriers to ensure American businesses and workers can compete on an even playing field within foreign markets.[78] The Secretary stated that in order to fulfill this goal, ITA will defend U.S. workers by addressing

[77] Office of the United States Trade Representative, Executive Office of the President, March 2021. *2021 Trade Policy Agenda and 2020 Annual Report of the President of the United States on the Trade Agreements Program.* Washington, DC: USTR. Available online at https://ustr.gov/sites/default/files/files/reports/2021/2021%20Trade%20Agenda/Online%20PDF%202021%20Trade%20Policy%20Agenda%20and%202020%20Annual%20Report.pdf (accessed July 16, 2021).

[78] *Responses to Questions for the Record for Governor Gina Raimondo, Nominee to be Secretary of Commerce Before the Senate Commerce Committee*, January 26, 2021. Available online at https://www.commerce.senate.gov/services/files/A5815F7A-E1D8-4F44-ACE6-4B7B093B299B (accessed July 20, 2021).

unfair foreign trade practices and barriers, strengthening enforcement of U.S. trade laws, and enhancing oversight of foreign government compliance with trade agreements.[79]

To address the Secretary's and Administration's priorities, we initiated an audit[80] in FY 2021 to assess ITA's actions taken to remove and reduce foreign trade barriers.

Protecting national security through effective enforcement of export controls

BIS administers and enforces the Export Administration Regulations (EAR) over foreign and U.S. companies as well as over individuals, regardless of their location or nationality, pursuant to the Export Control Reform Act of 2018.[81] The EAR apply to dual-use items (commodities, software, and technology), as well as to purely commercial items and to various military items, to prevent exports and reexports (and, in certain instances, in-country transfers) of sensitive items to embargoed and sanctioned destinations, to prohibited end users, and for prohibited end uses. The EAR also ensure parties involved in U.S. commercial transactions do not engage in prohibited foreign boycott activities. The Export Control Reform Initiative[82] brought about a number of changes to the EAR and BIS operations, including the transfer of jurisdiction concerning thousands of items from the U.S. Munitions List (USML) to the Commerce Control List (CCL), as well as the ability to export and reexport to eligible countries under license exception certain CCL items that had formerly been munitions items on the USML.[83] These changes increased BIS' licensing workload from 33,615 license applications processed in FY 2016 to 37,895 applications processed in FY 2020—a 12.7 percent increase.[84] Of the licenses processed in FY 2020, 12,400—or 32.7 percent—were for items transferred from the USML to the CCL.[85]

---

[79] *Statement of Gina M. Raimondo, Secretary, U.S. Department of Commerce, Before the House Committee on Appropriations, Subcommittee on Commerce, Justice, Science and Related Agencies*, May 6, 2021. Available online at https://docs.house.gov/meetings/AP/AP19/20210506/112566/HHRG-117-AP19-Wstate-RaimondoG-20210506.pdf (accessed July 20, 2021).

[80] DOC OIG, July 16, 2021. *Audit of ITA's Efforts to Resolve Foreign Trade Barriers,* #2021-410. Washington, DC: DOC OIG.

[81] Pub. L. No. 115-232. The Export Control Reform Act of 2018 is the permanent statutory authority for EAR. The EAR are found in 15 C.F.R. Parts 730-774 (2021).

[82] The Export Control Reform Initiative, which began in April 2010, was a three-phase effort initiated under former President Obama's administration to streamline the nation's export control system. See White House. *Fact Sheet on the President's Export Control Reform Initiative* [online]. https://obamawhitehouse.archives.gov/the-press-office/fact-sheet-presidents-export-control-reform-initiative (accessed July 16, 2021).

[83] For information on the License Exception Strategic Trade Authorization, see 15 C.F.R. 740.20 (2021), *License Exception Strategic Trade Authorization*, and *Supplement No. 1 to Part 740—Country Groups* (Country Group A, columns A:5 and A:6 (listing the eligible countries)).

[84] DOC Bureau of Industry and Security, January 21, 2021. *Annual Report to Congress for Fiscal Year 2020*. Washington, DC: DOC BIS, p. 9. Available online at https://www.bis.doc.gov/index.php/documents/pdfs/2711-2020-bis-annual-report-final/file (accessed July 16, 2021).

[85] *Ibid.*

To be effective, export controls must be enforced, and companies or individuals who illegally export EAR-controlled items, including through evasion and circumvention, must be detected and prosecuted accordingly. With greater responsibilities overseeing many more items under its jurisdiction, BIS must ensure it enforces the EAR and pursues action against violators.

Progress made/challenges remaining since the FY 2021 TMC

In our FY 2021 *Top Management Challenges* report, we highlighted as a priority area "evaluating and improving processes for adjudicating Section 232 exclusion requests."[86] In FY 2021, we completed our audit of the exclusion request process to determine whether (1) BIS and ITA adhered to the established processes and procedures to review exclusion requests and (2) decisions on requests were reached in a consistent and transparent manner. We found that (1) U.S. companies were denied exclusion requests based on incomplete and contradictory information, and (2) the Section 232 exclusion request review process lacked transparency.[87] We made recommendations to both BIS and ITA. We received concurrence on most of our recommendations, and both bureaus have taken or will take actions to implement them.

[86] OIG-21-003, p. 26.

[87] DOC OIG, January 25, 2021. *Decisions on Exclusions from Section 232 Tariffs Were Not Transparent and Based on Incomplete and Inaccurate Information*, OIG-21-020-A. Washington, DC: DOC OIG.

Challenge 5: Establishing a Strong Framework for Designing the 2030 Census and Improving Operations over Surveys and Employee Background Investigations

In 2020, the Census Bureau carried out the 24th Decennial Census, as mandated by the U.S. Constitution.[88] The Census Bureau announced on April 26, 2021, that the U.S. resident population in the 50 states and the District of Columbia was 331,449,281 as of April 1, 2020.[89] The data derived from this Decennial Census will be used to reapportion the 435 seats among the respective states in the House of Representatives and redraw Congressional districts. Decennial Census data will also be used to determine the allocation of $675 billion in federal funding. However, the COVID-19 pandemic forced the Census Bureau to make major and unprecedented adjustments to its plans, such as suspending key census operations and modifying its approach to data collection.

The Decennial Census funding lifecycle is normally a 12-year period that overlaps with the prior census. The 2020 Decennial Census funding lifecycle started in FY 2012 and will end in FY 2023. However, given the challenges of 2020, some late activities related to 2020 operations are now scheduled to end in FY 2025 rather than late in FY 2024 as previously planned. In preparation for the 2030 Decennial Census lifecycle, the Census Bureau is in the process of evaluating and assessing 2020 Census operations. This effort is critically important in laying the groundwork for improving innovations used during the 2020 Census.

OIG's FY 2022 top management and performance challenges include these priority areas related to the census:

- Ensuring data collection is high quality
- Ensuring advertising efforts increase response rates
- Ensuring only candidates suitable for federal government employment are hired

Ensuring data collection is high quality

The 2020 Census faced unprecedented obstacles—such as the COVID-19 pandemic and natural disasters—resulting in the Census Bureau making last-minute changes to its operational design. These last-minute changes have raised concerns regarding their impact on data collection and resulting data quality. In response, the Census Bureau published on its website detailed state-level quality metrics for public consumption and sought the assistance of outside groups to independently assess data quality. Such data include the nonresponse followup proxy[90] rate, which for occupied housing in 2020 was 26 percent—slightly higher than the rate

[88] U.S. Const. art. 1, § 2.

[89] DOC U.S. Census Bureau, April 26, 2021. *2020 Census Apportionment Results Delivered to the President*, Release Number CB21-CN.30. Suitland, MD: DOC Census. Available online at https://www.census.gov/newsroom/press-releases/2021/2020-census-apportionment-results.html (accessed June 29, 2021).

[90] According to the Census Bureau, "[i]f high-quality administrative records aren't available for an address after an initial visit, census takers continue to visit the address. If they still can't get a response after three visits, they try to

of nearly 25 percent in 2010.[91] To address stakeholder concerns about data quality and ensure that lessons learned from the 2020 Census inform the next Decennial Census, the Census Bureau should ensure its 2020 Census Evaluations and Experiments studies are completed on time and adhere to the Census Bureau's *Statistical Quality Standards*.[92]

Data quality is also a concern with ongoing surveys conducted by the Census Bureau. For instance, in recent years the Census Bureau has reported a decline in response rates for the Current Population Survey[93] and other household surveys. Consequently, in FY 2022, the Census Bureau plans to embark on an initiative to determine whether the Current Population Survey can be conducted using an Internet self-response instrument in addition to the established approach of conducting interviews with respondents in person and via telephone. Given the potential for Internet self-response to improve—or at least prevent a decline in—response rates, the Census Bureau should ensure this initiative begins and is completed on schedule.

Our ongoing evaluation assesses the adequacy of the Census Bureau's quality control processes to ensure the data collected during the 2020 Census was complete and accurate. [94] The results of this evaluation will provide lessons learned to the Census Bureau as it assesses the impact of design changes and operational challenges in 2020 to inform planning for the 2030 Census.

Ensuring advertising efforts increase response rates

The Census Bureau budgeted more than $500 million for public education and an outreach campaign that was designed to increase 2020 Census response rates. As the Census Bureau prepared for and conducted the 2020 Census, it faced a challenging set of environmental factors such as declining response rates, an increasingly diverse population, and more informal and complex living arrangements. In order to increase self-response rates, the Census Bureau promoted self-response by taking advantage of new technologies. Paid advertising was first used by the Census Bureau during the 2000 Census and appears to have stopped a declining response rate, which was 65 percent for both the 1990 and 2000 censuses. In the 2010 Census, the Census Bureau's Integrated Communications Program was developed in an effort to build

---

get information about the address from a neighbor, landlord or building manager. We refer to these as 'proxy responses.' We also rely on these types of proxies to help us verify housing units that appear vacant or cannot be located." *See* DOC Census Bureau. *How We Complete the Census When Households or Group Quarters Don't Respond* [online]. https://www.census.gov/newsroom/blogs/random-samplings/2021/04/imputation-when-households-or-group-quarters-dont-respond.html (accessed August 26, 2021).

[91] DOC Census Bureau, April 26, 2021. *Census Bureau Releases Quality Indicators on 2020 Census*, Release Number CB21-CN.29. Suitland, MD: DOC Census; *see* "Operational Metrics," "Downloadable Table." Available online at https://www.census.gov/newsroom/press-releases/2021/quality-indicators-on-2020-census.html (accessed June 20, 2021).

[92] DOC Census Bureau, July 2013. *U.S. Census Bureau Statistical Quality Standards*. Suitland, MD: DOC Census. Available online at https://www.census.gov/content/dam/Census/about/about-the-bureau/policies_and_notices/quality/statistical-quality-standards/Quality_Standards.pdf (accessed August 26, 2021).

[93] The Current Population Survey is the primary source of labor force statistics for the U.S. population and is jointly sponsored by the U.S. Department of Labor and the Census Bureau.

[94] DOC OIG, November 3, 2020. *Evaluation of 2020 Census Data Quality Processes*, #2021-386. Washington, DC: DOC OIG.

on the success of the 2000 Census program. However, the self-response rate remained at 65 percent. The 2020 Census Integrated Partnership and Communications Campaign, conducted as a contracted service, was one of the most extensive and far-reaching marketing campaigns ever conducted by the federal government; however, even with the ability to respond via the Internet, the response rate remained at 65 percent. Although demonstrating a direct causal link between the contractor's activities and achieving the objective of increasing response rates is difficult, the Census Bureau's monitoring of the contractor's advertising efforts to ensure advertising costs achieved the desired outcome was important.

In order to assess whether the 2020 advertising contract achieved its goals, we will be conducting an audit during FY 2022 to determine whether the Census Bureau's actions overseeing the contract were sufficient for ensuring contract outcomes were achieved.

Ensuring only candidates suitable for federal government employment are hired

Census Investigative Services (CIS) plays a key role in the hiring process at the Census Bureau. CIS staff is responsible for conducting pre- and post-employment adjudication (if required) for all Census Bureau employees and contractors. The information CIS staff reviews is sensitive, and a failure to conduct a review and adjudicate investigations per Census Bureau and U.S. Office of Personnel Management requirements could result in the hiring of candidates that are not suitable for federal employment.

Our prior reviews of CIS have identified significant problems with the office:

- In response to a Congressional request, we observed that CIS staff did not conduct a background investigation in accordance with requirements and, as a result, the Census Bureau hired a registered sex offender to work at one of its area Census offices.[95] After working for the Census Bureau for several months, the employee was arrested again and their employment was terminated in March 2019.
- Additional concerns were raised when it was determined that CIS, at the direction of Census Bureau management, was not conducting post-employment adjudication of investigations, which resulted in additional employees with derogatory background information continuing to work for the Census Bureau.[96] We found that the Census Bureau had not adjudicated more than 10,000 background investigations, some of which dated back to 2014. More than a dozen individuals with derogatory information in their background investigations had access to Census Bureau facilities and information systems for 4 or more years, and some of these individuals have positions the Census Bureau has deemed "high-risk" or "critical," including some working in the IT field.

[95] DOC OIG, December 10, 2019. *IG Letter to NC Delegation: the Census Bureau's Background Check and Hiring Process*, OIG-20-012-M. Washington, DC: DOC OIG.

[96] DOC OIG, April 30, 2020. *Management Alert: The Census Bureau Has Not Adjudicated Hundreds of Individuals Identified as Highest-Risk in OPM Background Investigations*, OIG-20-023-M. Washington, DC: DOC OIG.

- We issued a management alert[97] concluding that the Census Bureau did not effectively restrict and monitor Census Hiring and Employment Check system roles and privileges in order to ensure that access was based on a valid authorization and limited to only what was required to accomplish assigned duties. Additionally, some staff had access to sensitive background investigation information before completion of their own required background check. The lack of internal controls increases the risk that unauthorized users will gain access to sensitive information.

While the Census Bureau has made progress in reducing its backlog of unadjudicated post-employment cases, it must also address the aforementioned deficiencies. In addition, the Census Bureau must process new cases that it continued to receive while it focused on clearing the backlog. If these issues are not addressed, individuals who are unsuitable for federal employment may be hired or be allowed to continue their employment, placing the Census Bureau's facilities and systems—and possibly the public—at risk.

In addition, our ongoing CIS Background Investigation Processing evaluation will determine whether CIS is processing background investigations in a manner that reduces the risk of hiring unsuitable employees and ensures the security of sensitive information.

Progress made/challenges remaining since the FY 2021 TMC

The Census Bureau made progress in meeting the revised deadline of April 30, 2021, for releasing the apportionment data; however, it continues to face challenges as noted in the FY 2021 *Top Management Challenges* report. For instance, the Census Bureau is facing challenges in the following critical areas:

Ensuring an accurate count

On October 15, 2020, the Census Bureau completed its field enumeration of the U.S. population. The Census Bureau is working with outside entities to assess data accuracy and will continue its internal assessments and evaluations of 2020 Census operations.

During the Census Bureau's 2020 Census operations, we issued a report and a series of management alerts that identified serious weaknesses in areas that could create increased risk for a complete and accurate 2020 Census. After completion of the Address Canvassing operation, we issued an alert that highlighted internal control weaknesses over the tracking and collection of laptop devices.[98] During nonresponse followup, we issued management alerts that

[97] DOC OIG, December 1, 2020. *Management Alert: The Bureau Cannot Ensure That Access to Sensitive Background Investigation Information Is Limited to Individuals Who Have a Work-Related Need to Know*, OIG-21-011-M. Washington, DC: DOC OIG.

[98] DOC OIG, August 13, 2020. *Management Alert: The Census Bureau Cannot Account for the Return of All Devices Used During 2020 Decennial Census Field Operations*, OIG-20-040-M. Washington, DC: DOC OIG.

highlighted concerns in the areas of hiring,[99] college and university student counts,[100] personal protective equipment,[101] resolving alerts,[102] employee awards,[103] and the reinterview process.[104] We are currently assessing the adequacy of the Census Bureau's quality control processes to ensure the data collected during the 2020 Census was complete and accurate.

Ensuring that lessons learned from the 2020 Census are an essential part of success in 2030 and assessing 2020 Census successes and areas needing improvement

With enumeration operations concluded, the Census Bureau is in the process of completing and carrying out experiments, evaluations, and assessments of the 2020 Census through the Evaluations and Experiments operation. The Census Bureau will release these studies on a rolling basis until the operation is completed in FY 2024.

Developing a testing schedule that ensures completion of tests as planned and anticipates funding needs

In its FY 2022 budget justification, the Census Bureau requested resources to begin its 2030 Census planning efforts. Specifically, it plans to initiate research into optimizing the following areas of the 2020 Census: updating and maintaining the address list, leveraging administrative records to reduce nonresponse followup, and continuing to reduce the physical footprint. This research will help in developing plans for the next Decennial Census. As with the 2020 Census, a period of research is undertaken to determine the type and level of testing that will be required, which in turn will be used to finalize a field testing schedule.

Ensuring only candidates suitable for federal government employment are hired

During FY 2020 and FY 2021, we issued management alerts that identified serious weaknesses in areas that could put Census Bureau systems and facilities—as well as the public—at risk. Specifically, we reported that (1) the Census Bureau had a significant backlog in post-employment adjudications[105] and (2) the Census Bureau could not ensure that access to sensitive background investigation information was limited to individuals who had a work-related need to know.[106] In early FY 2021, the Census Bureau reported a significant decrease in

[99] DOC OIG, August 18, 2020. *2020 Census Alert: The Census Bureau Faces Challenges in Accelerating Hiring and Minimizing Attrition Rates for Abbreviated 2020 Census Field Operations*, OIG-20-041-M. Washington, DC: DOC OIG.

[100] DOC OIG, August 27, 2020. *2020 Census Alert: The Census Bureau May Not Accurately Count College and University Students Living Off-Campus During the 2020 Census*, OIG-20-044-M. Washington, DC: DOC OIG.

[101] DOC OIG, September 8, 2020. *2020 Census Alert: The Census Bureau Faces Challenges in Ensuring Employee Health Safety During 2020 Census Field Operations*, OIG-20-046-M. Washington, DC: DOC OIG.

[102] DOC OIG, September 17, 2020. *2020 Census Alert: Delays to Resolving Alerts Limit the Bureau's Ability to Maintain or Improve the Quality of 2020 Census Data*, OIG-20-048-M. Washington, DC: DOC OIG.

[103] DOC OIG, September 28, 2020. *2020 Census Alert: The Census Bureau's Program to Provide Awards to Nonresponse Followup Enumerators and Field Supervisors May Require Additional Quality Assurance of Cases to Ensure Data Accuracy*, OIG-20-052-M. Washington, DC: DOC OIG.

[104] DOC OIG, December 28, 2020. *2020 Census Alert: Inability to Finish Nonresponse Followup RIs Raises Concerns Over the Quality of More Than 500,000 Cases*, OIG-21-015-M. Washington, DC: DOC OIG.

[105] OIG-20-023-M.

[106] OIG-21-011-M.

the number of background investigations pending post-employment adjudication. On September 2, 2020, the number of post-employment cases pending adjudication remained above 11,000, whereas on November 3, 2020, that number was reported at less than 250. We are currently conducting follow-up work to determine whether concerns with the processing of employee background investigations were resolved.

Challenge 6: Meeting Intellectual Property Stakeholder Needs in the Midst of Economic, Technological, and Legal Changes

Intellectual property (IP) is used in virtually every segment of the U.S. economy. IP-intensive industries support at least 45 million U.S. jobs—30 percent of all employment—and contribute 38.2 percent of U.S. gross domestic product.[107] U.S. innovators depend on USPTO to conduct high-quality, timely patent and trademark examinations to produce reliable and predictable IP rights that protect their new ideas and investments. As the economic, technological, and legal landscapes continue to change, USPTO faces challenges in meeting these stakeholders' needs.

OIG's FY 2022 top management and performance challenges include these priority areas related to USPTO:

- Improving efficiency, quality, and timeliness of patent decisions
- Ensuring proper use of the trademark system
- Managing performance of mission-critical services

Improving efficiency, quality, and timeliness of patent decisions

USPTO continues to face challenges in efficiently providing quality decisions in a timely manner. USPTO recently aligned its pendency goals with patent term adjustment (PTA) regulations.[108] It has also set its internal benchmark for 85 percent of examiner actions to be issued within PTA deadlines. In February 2021, USPTO reported that the percentage of all actions meeting those deadlines was in the mid- to high-80s. However, as of May 2021, first action pendency[109] was 17 months, a 2-year high.[110] USPTO recognizes that improvements are needed to process first office actions within 14 months. We recently published a report[111] noting that about half of issued patents receive PTA compensation, indicating that USPTO will continue to face challenges in meeting its pendency goals.

---

[107] United States Patent and Trademark Office. *Intellectual Property and the U.S. Economy* [online]. https://www.uspto.gov/learning-and-resources/ip-motion/intellectual-property-and-us-economy (accessed July 29, 2021).

[108] PTA compensates for delays caused by USPTO in issuing a patent by adding time to a patent's term. Particular delays are taking more than (1) 14 months to issue a first office action on an application, (2) 4 months to respond to an applicant's reply, or (3) 3 years to issue a patent. *See* 35 U.S.C. § 154(b); 37 C.F.R. § 1.703 (2021).

[109] First action pendency is the average number of months from the patent application filing date to the date USPTO mails a first office action. An office action on the merits commonly cites prior art and gives reasons why the examiner has allowed and/or rejected claims in the application and a first action on the merits is typically the first substantive examination by an examiner.

[110] USPTO's first action pendency is the average over a 3-month period, and its calculation of PTA compliance for all mailed actions is based on year-to-date results.

[111] DOC OIG, July 6, 2021. *USPTO Has Opportunities to Improve its Internal Controls and Oversight Related to PTA and PTE Calculations*, OIG-21-030-I. Washington, DC: DOC OIG. *Note*: Our office contracted with The MITRE Corporation—an independent firm—to perform this evaluation.

As the U.S. economy recovers from the COVID-19 pandemic, USPTO patent examination workloads may increase substantially. In May 2021, USPTO announced that patent filings were not as low as originally expected.[112] With improved economic conditions, an increasing trend in patent filings can be expected. Accordingly, USPTO may face further patent pendency challenges from an increased workload. USPTO plans to enlarge the examiner corps by approximately 8 percent to help reduce pendency, but hiring, training, and supervising those new examiners will require an investment of time and resources.

USPTO also continues to face challenges in maintaining and improving the quality of patent examination. Its Office of Patent Quality Assurance (OPQA) analyzes a selection of examiners' office actions to measure conformity with four principal statutes governing patentability.[113] In one example, OPQA's assessment in the 2nd quarter of FY 2021 found 83 percent of rejections for obviousness to be compliant with the statute. USPTO's goal for this statute is to be at least 93 percent compliant.[114] USPTO is implementing a new Time, Routing, and Performance plan to give examiners more time toward better-quality patent decisions. However, that additional examination time risks increasing the number of actions that do not meet PTA timeliness goals. USPTO will continue facing challenges in balancing quality efforts with the PTA deadlines noted previously.

USPTO's adjudicative body, the Patent Trial and Appeal Board (PTAB), will also continue to face challenges. We recently issued a report identifying examples of PTAB's challenges in planning for staff needs and tracking case data.[115] While USPTO has reduced the pendency of appeals[116] since FY 2020, pendency has recently been leveling off or trending slightly upward.[117] A number of contested cases[118] were being held in abeyance pending the Supreme Court's recent *Arthrex* decision[119] on the status and authority of PTAB's administrative patent judges.

---

[112] In May 2021, USPTO revised its projection for patent filings to be reduced only by 2 percent for FY 2021. For FY 2022, USPTO forecasts a filing increase of about 1.5 percent.

[113] These statutes are 35 U.S.C. § 101 (eligible subject matter), § 102 (novelty), § 103 (nonobviousness), and § 112 (adequate description).

[114] USPTO set this 93 percent goal for overall nonobviousness compliance (i.e., including both rejections and actions for which no obviousness rejection was made). As of the end of the 2nd quarter of FY 2021, overall compliance in this context was below the goal, at 90.6 percent. USPTO does not have a separate goal for rejection compliance.

[115] DOC OIG, May 10, 2021. *The PTAB Faces Operational, Information Technology, and Data Risks*, OIG-21-025-I. Washington, DC: DOC OIG. *Note*: Our office contracted with The MITRE Corporation—an independent firm—to perform this evaluation.

[116] These are appeals of examiner rejections of claims in a patent application. An applicant, "any of whose claims has been twice rejected," may appeal to the PTAB. *See* 37 C.F.R. § 41.31 (2021).

[117] Statistics for May 2021 showed an average pendency of 13.2 months for the March to May 2021 period, which is a significant improvement over the same period in 2020 (15.4 months), but remains above PTAB's goal of 12 months and is an increase over the period from November 2020 to January 2021 (13 months).

[118] Contested cases include inter partes reviews, post-grant reviews, and derivations. *See* 37 C.F.R. Part 41, Subpart D and Part 42 (2021).

[119] *United States v. Arthrex, Inc.*, 594 U.S. ___, 141 S. Ct. 1970 (2021).

Processing these cases alongside new contested cases will pose a challenge to PTAB's ability to meet statutory deadlines.

The *Arthrex* holding enabled the Under Secretary of Commerce for Intellectual Property and Director of USPTO (Director) to review and revise PTAB decisions in contested cases. USPTO must now develop policy, procedures, and/or regulations for the Director to exercise this discretion based on ongoing PTAB caseload and statutory pendency requirements. In June 2021, USPTO announced and sought comments on initial measures and a policy for Director review of PTAB decisions. USPTO will need to incorporate this feedback and devote resources to implementing the new procedures. Moreover, the initial procedures were challenged in court almost as soon as they were announced. Further disputes regarding the Director's review policies and procedures will present additional litigation workload for USPTO.

Ensuring proper use of the trademark system

In our FY 2021 *Top Management Challenges* report, we noted that USPTO had implemented new rules and examination guidance to address fraudulent or inaccurate trademark filings, but continued to face challenges from filers attempting to circumvent the requirements of trademark laws and regulations.[120] Since that report, we completed an audit of these initiatives and found that USPTO continues to face challenges in this area. In our audit report,[121] we determined that USPTO's efforts were ineffective at preventing fraudulent or inaccurate registrations. Specifically, we found that USPTO (1) lacked controls to effectively enforce the U.S. counsel rule, (2) approved trademark filings with digitally altered or mocked-up specimens, (3) did not ensure accurate identification of goods and services, and (4) lacks a comprehensive fraud risk strategy. We made recommendations for USPTO to improve its policies and procedures to prevent and detect fraudulent or inaccurate trademark filings.

Concerns about fraudulent or inaccurate filings are heightened by a large increase in filings from China, from which many applications with inaccurate claims of use have originated. In the 4th quarter of 2020, 38 percent of all applications received originated from China, up from 9 percent in the same period of 2019. Recently, USPTO's Office of Enrollment and Discipline issued a final order suspending a Beijing-based attorney who did not follow USPTO rules in filing several hundred registration applications. According to the Commissioner of Trademarks, as of June 17, 2021, the number of trademark applications was 63 percent higher than in FY 2020. The number of pending applications grew 31 percent from the 2nd quarter of FY 2020 to the 2nd quarter of FY 2021. First action pendency increased from 2.7 months to 4.7 months in the same period. Given the growing backlog of trademark applications, USPTO has estimated that it will not be able to return to historical pendency targets until FY 2025.

At the same time, USPTO must implement the Trademark Modernization Act of 2020 (TMA),[122] which was enacted in December 2020. The TMA creates new proceedings to cancel unused trademarks and provides additional grounds for cancellation of unused trademarks at

[120] OIG-21-003, p. 21.

[121] DOC OIG, August 11, 2021. *USPTO Should Improve Controls over Examination of Trademark Filings to Enhance the Integrity of the Trademark Register*, OIG-21-033-A. Washington, DC: DOC OIG.

[122] Pub. L. No. 116-260, Division Q, Title II, Subtitle B (2020).

the Trademark Trial and Appeal Board. USPTO published proposed rules to implement those proceedings and to change the time to respond to office actions in May 2021, and must finalize the rules by December 2021. The TMA should help address the problem of inaccurate trademark filings by removing unused marks from the trademark register. However, USPTO will face challenges as it implements the TMA, including balancing stakeholder perspectives and addressing potential workload increases.

Managing performance of mission-critical services

Over the past few years, we have identified the modernization of USPTO's legacy IT systems as a top management and performance challenge.[123] USPTO continues to face challenges in stabilizing and modernizing all of its legacy systems to minimize the risk of system failures. Since FY 2011, USPTO has been developing and modernizing its outdated patent legacy systems and replacing them with next-generation systems. USPTO's goal was to retire the patent legacy systems no later than FY 2013; however, USPTO did not meet that goal because the IT modernization effort has not progressed as quickly as planned. Only four legacy systems have been retired to date, and USPTO plans to retire nine additional legacy systems by FY 2023—10 years later than originally planned.

In January 2020, USPTO began rolling out its "New Ways of Working" (NWOW) initiative. The goals of the initiative are to (1) increase collaboration, (2) deliver value to the business, (3) empower teams, and (4) foster continuous improvements through increased feedback. However, as noted in a recent report concerning PTAB,[124] USPTO faces challenges in adapting to the new process. For example, under the NWOW, the product owner is a member of the agile team who serves as the proxy for the end user and is responsible for prioritizing product features and requirements. The report noted that the Office of the Chief Information Officer and PTAB provided conflicting information on who the product owner is for the PTAB End-to-End system. In its response to the report, USPTO indicated it has appointed a Lead Administrative Patent Judge as Acting Lead Product Owner. As USPTO continues to implement the NWOW, it is critical that it provide effective oversight of the process to ensure a timely and seamless transition to next-generation systems.

While USPTO works to replace aging systems, it also is adding technical capabilities. In our FY 2021 *Top Management Challenges* report, we noted that the adoption of artificial intelligence (AI) tools presented risks and operational challenges alongside potential benefits.[125] Since then, USPTO has continued to introduce and refine software containing AI components with the aim of (1) increasing efficiency in examination via automated classification and (2) improving thoroughness of prior art searching by expanding the range of available references and pointing examiners to relevant references. However, the search tool is as yet only in use by a segment of the examining corps, and the new AI algorithms used in these tools present the challenge of monitoring and adjusting them to better achieve the tools' purposes. USPTO is facing the

[123] See, e.g., (1) OIG-20-001, p. 17, and (2) OIG-21-003, pgs. 20–21.

[124] OIG-21-025-I.

[125] OIG-21-003, p. 20.

quantitative challenge of placing these tools in the hands of the entire examining corps as well as the qualitative challenge of ensuring they improve examination efficiency and legal compliance.

Over the past few years, we have reported on USPTO's challenges related to the management and oversight of its contracts.[126] USPTO relies on contractors for many of its core business functions, such as front-end processing, data capture, and publication of patent applications, as well as support for patent and trademark IT systems. USPTO spent more than $262 million on contractual services in FY 2020. In our recent audit[127] of USPTO's Software Development and Integration-Next Generation (SDI-NG) contract, we found that USPTO (1) did not timely plan and compete a follow-on SDI-NG contract and (2) did not document and use contractor performance information adequately. Reliance on a bridge contract for SDI-NG caused USPTO to incur costs of approximately $47 million that potentially could have been avoided by timely recompeting the contract when it expired. It is therefore critical that USPTO improve its processes to award and manage its contracts to ensure that contractors are performing adequately and costs are validated and controlled.

Progress made/challenges remaining since the FY 2021 TMC

Despite temporary declines in trademark applications due to the COVID-19 pandemic, USPTO saw an overall increase in trademark applications in FY 2021. Fee collections for new applications and renewals exceeded USPTO's projections, and USPTO projected that its trademark operating reserve would remain above its minimum level into FY 2022. USPTO also delayed implementation of its updated patent fee schedule to assess the impact of the COVID-19 pandemic on projected fee collections, and concluded that the patent operating reserve will maintain an acceptable balance. However, USPTO has projected that the economic effects of the COVID-19 pandemic will continue to affect patent filings at least into FY 2022. This uncertainty will present challenges, as USPTO must ensure that financial resources are sufficient to support operational needs.

[126] See (1) DOC OIG, July 10, 2019. *USPTO Could Improve Oversight Practices to Close Out Contract Files by Complying with Acquisition Regulations and Policies*, OIG-19-018-A. Washington, DC: DOC OIG; (2) DOC OIG, September 1, 2020. *USPTO Needs to Improve Its Small Business Contracting Practices*, OIG-20-045-A. Washington, DC: DOC OIG; and (3) DOC OIG, November 19, 2020. *USPTO Should Improve Acquisition Planning and Vendor Performance Management to Prevent Schedule Delays and Unnecessary Costs Related to the SDI-NG Contract*, OIG-21-010-A. Washington, DC: DOC OIG.

[127] OIG-21-010-A.

Challenge 7: Deploying a Nationwide Public Safety Broadband Network

The Middle Class Tax Relief and Job Creation Act of 2012 (the Act) established FirstNet Authority as an independent authority within NTIA to ensure the building, deployment, and operation of an NPSBN dedicated to first responders. On March 28, 2017, FirstNet Authority entered into a 25-year indefinite-delivery, indefinite-quantity contract with the NPSBN contractor for the construction and operation of the NPSBN. FirstNet Authority's arrangement with the NPSBN contractor involves (a) an initial obligation of up to $6.5 billion in funds to the NPSBN contractor to deploy the NPSBN, (b) the NPSBN contractor's use of dedicated broadband spectrum, and (c) payments from the NPSBN contractor to FirstNet Authority over the life of the contract to support FirstNet Authority operations and for the construction, maintenance, operations, and improvement of the NPSBN.

OIG's FY 2022 top management and performance challenges include these priority areas related to FirstNet Authority:

- Ensuring a sound reinvestment process
- Ensuring the successful performance of the contract

FY 2022 is an important year, as the Act requires GAO to make a recommendation regarding what action Congress should take regarding FirstNet Authority's 2027 sunset of authority.[128] Also, the NPSBN contractor is required to meet important contract deliverables relating to adoption (e.g., connection targets).

Ensuring a sound reinvestment process

The NPSBN contractor makes required annual fixed payments[129] to FirstNet Authority. Of the $18 billion to be received over 25 years, approximately $15 billion is expected to be used for reinvestments. To date, FirstNet Authority received five payments totaling $600 million. In June 2020, the FirstNet Authority Board approved its first two reinvestments totaling $218 million for

- an increase of deployables capabilities, and
- a core upgrade to support initial 5G capabilities.

The $218 million amount is less than the total expected contract costs of the reinvestments. FirstNet Authority requested that our office not disclose the current total value for the task orders. FirstNet Authority views the value as Source Selection Data and a trade secret of the NPSBN contractor that has not been publicly disclosed.

[128] *Middle Class Tax Relief and Job Creation Act of 2012*, Pub. L. No. 112-96 § 6206(g).

[129] Although payment amounts are fixed, the amounts vary annually based on the NPSBN contract.

Reinvestment opportunities that satisfy first responders' needs must be generated, properly vetted, and implemented.[130] "The reinvestment process helps the FirstNet Authority:

- Select investment opportunities that will best support the evolving mission and risk-based needs of public safety;
- Evaluate the investment opportunity to ensure it addresses FirstNet Authority legal, financial, and program requirements for the investment; and
- Identify and analyze the investment opportunity costs and proposed benefits before a significant amount of funds are allocated."[131]

It is imperative that FirstNet Authority use a sound framework for its reinvestment decision-making process that is transparent, logical, and justified, and that supports the evolving mission and risk-based needs of public safety prior to approval of new investments costing billions of dollars. The need for a sound process intensifies as the investment funding significantly increases to the billion-dollar range starting in 2026. Ensuring that the reinvestments selected are the most appropriate investments to ensure the maintenance, operation, and improvement of the NPSBN is essential to FirstNet Authority. To address this challenge, we are currently auditing the reinvestment process that FirstNet Authority used to select the investments.[132]

Ensuring the successful performance of the contract

Ensuring the successful performance of the complex NPSBN contract, one that includes payments to and from the NPSBN contractor, remains a challenge. FirstNet Authority must (1) ensure that procurement rules and regulations are followed and (2) provide proper oversight to verify that the NPSBN contractor meets contract requirements.

Both OIG and GAO have previously raised concerns with FirstNet Authority's administration of the contract. In January 2021, we identified persistent issues with FirstNet Authority's contract oversight.[133] We also raised concerns in August 2019 about senior management making unauthorized contract commitments, adding contract requirements, and improperly attempting to control contractor hiring decisions and manage contractor employee actions.[134] FirstNet Authority has been responsive to recommendations in our audit reports, taking a number of corrective actions. In January 2020, GAO reported that FirstNet Authority lacked a

[130] Section 6208(d) of the Act requires that FirstNet Authority reinvest fees received into the NPSBN only for the purposes of "constructing, maintaining, operating, or improving the network."

[131] First Responder Network Authority, July 1, 2021. *FirstNet Authority Investment Procedures*, FNPS 900-1. Reston, VA: FirstNet Authority. (Internal Department document.)

[132] DOC OIG, September 9, 2020. *Audit of FirstNet Authority's Reinvestment Process*, #2020-381. Washington, DC: DOC OIG.

[133] DOC OIG, January 5, 2021. *Continued FirstNet Authority Management Attention is Needed to Address Control Environment Weaknesses*, OIG-21-016-1. Washington, DC: DOC OIG.

[134] DOC OIG, August 1, 2019. *Management Alert: FirstNet Management Altered Contract Requirements Without Authorization*, OIG-19-020-M. Washington, DC: DOC OIG.

reliable master schedule to review.[135] FirstNet Authority expects to address the issue by the end of 2021.

Per the NPSBN contract, a key milestone will occur during the coming year. By March 2022, the contractor must meet 100 percent of the connection targets contained in Task Order 4. Our review of reports identifying current device connections by state shows the NPSBN contractor is at risk of not meeting state-specific connection goals. As the NPSBN is to be a nationwide network, FirstNet Authority needs to closely monitor the contract performance with respect to state-by-state connection totals. FirstNet Authority management must focus on contractor oversight, as failure to do so could result in the government not receiving the goods and services paid for and create a potential environment for fraud, waste, and abuse. To address this challenge, we plan to initiate an audit in FY 2022 to evaluate contractor performance involving connection target requirements.

Progress made/challenges remaining since the FY 2021 TMC

FirstNet Authority continues to make progress implementing the NPSBN. At its August 18, 2021, board meeting, FirstNet Authority reported that (1) the NPSBN was being used by more than 17,000 public safety agencies via more than 2.5 million device connections; (2) the NPSBN maintained an inventory of more than 100 dedicated deployable network assets; (3) more than 170 unique applications had been approved for listing in the application catalog; and (4) the NPSBN contractor made significant progress in the deployment of Band 14 coverage (approximately 90 percent). Also, in August 2021, FirstNet Authority reported that it continued to have extensive engagement with public safety agencies and users across the country, holding 463 engagements and reaching more than 11,000 stakeholders in the 3rd quarter of FY 2021.

FirstNet Authority was responsive to our January 2021 audit report[136] and provided an action plan to address the recommendation. FirstNet Authority has also been responsive to the challenges described in the FY 2021 *Top Management Challenges* report;[137] however, challenges continue due to the need for a sound reinvestment process, the extended contract period, and the addition of new task orders.

[135] GAO, January 27, 2020. *Public-Safety Broadband Network: Network Deployment Is Progressing, but FirstNet Could Strengthen Its Oversight*, GAO-20-346. Washington, DC: GAO.

[136] OIG-21-016-I.

[137] OIG-21-003, pgs. 12–17.

Appendix A: Related OIG Publications

This list presents OIG's FY 2021 work related to top management and performance challenges facing the Department in FY 2022. 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: Improving the Department's Cybersecurity Resiliency

- *The U.S. Census Bureau's Mishandling of a January 2020 Cybersecurity Incident Demonstrated Opportunities for Improvement* (OIG-21-034-A; August 16, 2021)

Challenge 2: Maintaining Continuity, Managing Risks, and Leveraging Investments to Improve Satellite Data, Products, and Services

- *The Department Has Made Progress Meeting Its Responsibilities Under the Geospatial Data Act But Must Improve Controls to Ensure Full Compliance* (OIG-21-001-A; October 1, 2020)

Challenge 3: Addressing Departmental Management Matters Involving Acquisitions and Grants

- *EDA Is Not Fully Complying with All Its Disaster Relief Award Policies* (OIG-21-014-A; December 21, 2020)
- *EDA Was Effective in Implementing the Requirements for Awarding Funds Under the CARES Act* (OIG-21-017-I; January 5, 2021)
- *2021 Annual Letter to OMB re: Government Charge Card Abuse Prevention Act of 2012* (OIG-21-022-M; January 29, 2021)
- *Management Alert: BAS Program's Focus on Technology May Overlook Risks Related to Business Processes* (OIG-21-023-M; April 19, 2021)
- *Audit of National Institute of Standards and Technology Working Capital Fund For Fiscal Year Ended September 30, 2019* (OIG-21-024-A; May 3, 2021)
- *OMAO Must Define and Implement a Disciplined Requirements Management Process to Ensure Future Acquisitions Meet User Needs* (OIG-21-027-I; May 25, 2021)
- *NOAA Fisheries Implemented the Requirements for Awarding Funds Under the CARES Act but Faces Challenges with the Pace of Funds Disbursement to Fishery Participants* (OIG-21-028-I; June 9, 2021)
- *NIST Was Effective in Implementing the Requirements for Awarding Funds Under the CARES Act* (OIG-21-032-I; August 5, 2021)

Challenge 4: Enhancing Capacity to Enforce Fair and Secure Trade

- *Decisions on Exclusions from Section 232 Tariffs Were Not Transparent and Based on Incomplete and Inaccurate Information* (OIG-21-020-A; January 25, 2021)

- *The U.S. & Foreign Commercial Service 2018 Officer Promotion Process Did Not Comply With Applicable Criteria* (OIG-21-021-I; January 28, 2021)

Challenge 5: Establishing a Strong Framework for Designing the 2030 Census and Improving Operations over Surveys and Employee Background Investigations

- *Management Alert: The Bureau Cannot Ensure That Access to Sensitive Background Investigation Information Is Limited to Individuals Who Have a Work-Related Need to Know* (OIG-21-011-M; December 1, 2020)
- *2020 Census Alert: Inability to Finish Nonresponse Followup RIs Raises Concerns Over the Quality of More Than 500,000 Cases* (OIG-21-015-M; December 28, 2020)
- *Fundamental Security Safeguards Were Not In Place to Adequately Protect the IT Systems Supporting the 2020 Census* (OIG-21-018-A; January 7, 2021)
- *IG Letter to Majority Leader Charles Schumer and Chairwoman Carolyn Maloney re: OIG Case No. 19-0728* (July 15, 2021)

Challenge 6: Meeting Intellectual Property Stakeholder Needs in the Midst of Economic, Technological, and Legal Changes

- *USPTO Should Improve Acquisition Planning and Vendor Performance Management to Prevent Schedule Delays and Unnecessary Costs Related to the SDI-NG Contract* (OIG-21-010-A; November 19, 2020)
- *The PTAB Faces Operational, Information Technology, and Data Risks* (OIG-21-025-I; May 10, 2021)
- *USPTO Has Opportunities to Improve Its Internal Controls and Oversight Related to PTA and PTE Calculations* (OIG-21-030-I; July 6, 2021)
- *USPTO Should Improve Controls over Examination of Trademark Filings to Enhance the Integrity of the Trademark Register* (OIG-21-033-A; August 11, 2021)

Challenge 7: Deploying a Nationwide Public Safety Broadband Network

- *Continued FirstNet Authority Management Attention is Needed to Address Control Environment Weaknesses* (OIG-21-016-I; January 5, 2021)

Appendix B: Acronyms and Abbreviations

ABI	Advanced Baseline Imager
Act	the Middle Class Tax Relief and Job Creation Act of 2012
AI	artificial intelligence
BAS	Business Applications Solutions
BIS	Bureau of Industry and Security
BPA	Blanket Purchase Agreement
CARES Act	Coronavirus Aid, Relief, and Economic Security Act
CCL	Commerce Control List
Census Bureau	U.S. Census Bureau
China	People's Republic of China
CIS	Census Investigative Services
CrIS	Cross-track Infrared Sounder
CRSRA	Commercial Remote Sensing Regulatory Affairs
Department	U.S. Department of Commerce
Director	Under Secretary of Commerce for Intellectual Property and Director of USPTO
DOD	U.S. Department of Defense
EAR	Export Administration Regulations
EDA	U.S. Economic Development Administration
eRA	Electronic Research Administration
ES	Enterprise Services
ESOC	Enterprise Security Operations Center
FCC	Federal Communications Commission
FirstNet Authority	First Responder Network Authority
FISMA	Federal Information Security Modernization Act of 2014
FY	fiscal year
GAO	U.S. Government Accountability Office
GEMS	Grants Enterprise Management System
GeoXO	Geostationary Extended Observations
GOES	Geostationary Operational Environmental Satellites
GPS	Global Positioning System

IP	intellectual property
IT	information technology
ITA	International Trade Administration
JPSS	Joint Polar Satellite System
LEO	low-earth orbit
NESDIS	National Environmental Satellite, Data, and Information Service
NIH	National Institutes of Health
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
NPSBN	Nationwide Public Safety Broadband Network
NPSBN contractor	AT&T
NTIA	National Telecommunications and Information Administration
NWOW	"New Ways of Working"
NWS	National Weather Service
OIG	Office of Inspector General
OMAO	Office of Marine and Aviation Operations
OMB	Office of Management and Budget
OPQA	Office of Patent Quality Assurance
OSC	Office of Space Commerce
PTA	patent term adjustment
PTAB	Patent Trial and Appeal Board
SCRM	supply chain risk management
SDI-NG	Software Development and Integration-Next Generation
STM	space traffic management
Suomi NPP	Suomi National Polar-orbiting Partnership
TMA	Trademark Modernization Act of 2020
TMC	Top Management Challenges
U.S.	United States
USML	U.S. Munitions List
USPTO	United States Patent and Trademark Office

011200000406