Top Management and Performance Challenges Facing the Department of Commerce in Fiscal Year 2023

FINAL REPORT NO. OIG-23-001
OCTOBER 13, 2022

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) 793-3336

DATE: October 13, 2022

CC: Don Graves, Deputy Secretary of Commerce
Eric Morrissette, Chief of Staff
André Mendes, Chief Information Officer
Jeremy Pelter, 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 2023***
Final Report No. OIG-23-001

The Office of Inspector General 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 2023.

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 Effectiveness Through Zero Trust

- Continuing to mature the information technology (IT) security program
- Transitioning to zero-trust architecture

Challenge 2: Ensuring Continuity of Environmental Data from Satellites, Ships, Aircraft, and Ground-Based Systems and Improving Weather and Climate Services

- Maintaining continuity of geostationary and polar satellites
- Developing the next generation of satellite systems
- Protecting observations, operations, and communications from frequency interference
- Moving toward an operational collision avoidance support service
- Recapitalizing ships and aircraft

[1] 31 U.S.C. § 3516(d).

- Balancing weather service improvements and longer-term climate resilience

Challenge 3: Managing IT Investments and Improving Supported Operations

- Avoiding further delays to Business Applications Solution implementation
- Managing risks to the implementation of an enterprise grants management system

Challenge 4: Ensuring Prudent Financial Management and Oversight of Broadband Infrastructure Funding

- Acquiring and maintaining sufficient staff with proficiency to ensure proper oversight and use of funds
- Implementing appropriate measures to prevent, detect, and report potential fraud and hold grantees, subgrantees, contractors, and subcontractors accountable for performance

Challenge 5: Enforcing Fair and Secure Trade and Effectively Implementing Export Controls

- Combating unfair trade practices by effectively resolving trade barriers and enforcing U.S. trade agreements
- Combating China's military-civil fusion strategy
- Ensuring proper implementation of export controls related to Russia's invasion of Ukraine

Challenge 6: Deploying a Nationwide Public Safety Broadband Network (NPSBN)

- Ensuring a sound reinvestment process
- Ensuring appropriate task order oversight
- Ensuring proper NPSBN adoption and coverage

Challenge 7: Improving Management and Oversight of Contracts and Grants to Ensure Responsible Spending

- Ensuring the integrity of grant programs
- Ensuring programs approved for State Small Business Credit Initiative funding comply with program requirements
- Developing and retaining a competent acquisition workforce to support the Department's mission

Challenge 8: Establishing a Strong Framework with Adequate Resources to Support the 2030 Census Planning Efforts and Enhance Overall Survey Quality

- Ensuring the timely delivery of 2020 Census studies and the timely completion of the *2020 Post-Census Group Quarters Review* needed to inform 2030 Census planning

- Ensuring information from the *Post-Enumeration Survey* is used to develop a strategy for obtaining a more accurate count of certain demographic groups and state populations for the 2030 Census
- Enhancing the accuracy and reliability of the U.S. Census Bureau's address list
- Ensuring data products provide timely, reliable, and quality data to stakeholders

Challenge 9: Strengthening U.S. Leadership in Intellectual Property

- Continuing efforts to improve and maintain patent quality and service
- Protecting and supporting registration processes and trademark owners
- Improving critical mission support functions

The final version of the report will be included in the Department's *Annual Financial Report*, as required by law.[2] 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. In addition to the topics included in the fiscal year 2023 top management and performance challenges report, we will review the Department's efforts to implement the CHIPS and Science Act (Pub. L. No. 117-167).

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) 793-3336.

[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 Effectiveness Through Zero Trust

Russia's February 2022 assault on Ukraine was not limited to kinetic attacks—it is a true full-scale cyber war.[1] However, Russia's cyberattacks are not limited to any specific geographical region. In fact, in the early days of the war, attacks against international satellite communication networks were attributed to Russian state-sponsored actors.[2] In expectation of a response to the unprecedented economic costs the U.S. and its allies imposed on Russia, the Cybersecurity & Infrastructure Security Agency (CISA) launched the "Shields Up" campaign.[3] As the U.S. Department of Commerce (the Department) is partially responsible for enforcing these sanctions, it is a potential target in this cyber war.

To combat ever-increasing cyberthreats, the President issued Executive Order 14028 in May 2021.[4] This order marked a dramatic change in the federal government's cybersecurity philosophy and moved the government toward zero-trust cybersecurity principles. This paradigm shift and its new security requirements will be particularly challenging for the Department, as it must simultaneously address longstanding cybersecurity weaknesses within its information technology (IT) security program.

The Office of Inspector General's (OIG's) fiscal year (FY) 2023 top management and performance challenges include these priority areas related to cybersecurity:

- Continuing to mature the IT security program
- Transitioning to zero-trust architecture

Continuing to mature the IT security program

To effectively address an ever-increasing number of cyber threats, the Department must ensure a healthy cybersecurity posture. Maturing its IT security program continues to be a top challenge for the Department in FY 2023. We have identified several key areas that will require prioritization from the Department.

---

[1] Atlantic Council, June 15, 2022. *Vladimir Putin's Ukraine invasion is the world's first full-scale cyberwar* [online]. https://www.atlanticcouncil.org/blogs/ukrainealert/vladimir-putins-ukraine-invasion-is-the-worlds-first-full-scale-cyberwar/ (accessed July 19, 2022).

[2] U.S. Department of Homeland Security Cybersecurity & Infrastructure Security Agency. *U.S. Government Attributes Cyberattacks on SATCOM Networks to Russian State-Sponsored Malicious Cyber Actors* [online]. https://www.cisa.gov/uscert/ncas/current-activity/2022/05/10/us-government-attributes-cyberattacks-satcom-networks-russian (accessed July 19, 2022).

[3] DHS CISA. *Shields Up* [online]. https://www.cisa.gov/shields-up (accessed July 19, 2022).

[4] 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 19, 2022).

Utilizing multifactor authentication (MFA) Department-wide

MFA has been promoted for use in the federal government since 2004.[5] Executive Order 14028 emphasized its value by requiring MFA to be implemented agency-wide by November 8, 2021. MFA's importance has continued to increase due to geopolitical tensions, and CISA has identified MFA as a key method to protect systems from attacks by nation-state actors.[6]

Although the November 2021 deadline has passed, the Department still faces barriers to fully implement MFA requirements. For example, the National Oceanic and Atmospheric Administration (NOAA) reported challenges with deploying MFA due to having scientific and specialized equipment in remote locations. The U.S. Census Bureau (Census Bureau) also stated that its mission requires voluntary cooperation from the public, which makes implementing MFA for external users a challenge. Further, we recently reported that none of the Department's national security systems[7] (NSS) had implemented MFA.[8]

As of January 2022, the Department reported that 76 percent of its systems have implemented MFA and that it has developed implementation plans for all systems that have yet to enforce MFA. However, these remaining systems must overcome significant obstacles to meet the goal of implementing MFA agency-wide.

Modernizing legacy systems

Our recent audit work found the Department continues to face challenges surrounding the use of outdated and unsupported technology. In our audit of the United States Patent and Trademark Office's (USPTO's) efforts to retire patent legacy systems,[9] we found that 49 servers were operating past their end of life (EOL), some by six years.[10] We also had a similar finding relating to the Department's NSS, in which we identified that an NSS had employed EOL

[5] DHS, August 27, 2004. *Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors*, ¶ 5. Washington, DC: DHS. Available online at https://www.dhs.gov/homeland-security-presidential-directive-12 (accessed July 19, 2022).

[6] DHS CISA, *Shields Up*.

[7] The National Institute of Standards and Technology describes an NSS as a system that stores, processes, or communicates classified information. See U.S. Department of Commerce National Institute of Standards and Technology, August 2003. *Guideline for Identifying an Information System as a National Security System*, NIST SP 800-59. Gaithersburg, MD: DOC NIST, page 9. Available online at https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-59.pdf (accessed August 18, 2022).

[8] DOC Office of Inspector General, June 15, 2022. *The Department Mismanaged, Neglected, and Wasted Money on the Implementation of IT Security Requirements for Its National Security Systems*, OIG-22-023-I. Washington, DC: DOC OIG.

[9] DOC OIG, July 20, 2022. *USPTO Needs to Improve Its Cost Estimating, Scheduling, and Agile Practices to Timely Retire Patent Legacy Systems*, OIG-22-026-A. Washington, DC: DOC OIG.

[10] Operating systems that reach EOL no longer receive support (e.g., security updates) from the manufacturer.

components.[11] Finally, our audit on NOAA's Active Directories identified EOL equipment being used to support critical NOAA enterprise services.[12]

Given these issues, we believe that the Department faces a pressing challenge to continue modernizing its legacy systems, including the replacement of EOL equipment. Keeping systems and their component equipment current is extremely important for security. CISA notes that "[c]ontinued use of EOL software poses consequential risk to your system[s] that can allow an attacker to exploit security vulnerabilities."[13] When hardware and software developers no longer support older legacy products, any security flaws discovered within those products become unmanaged and put systems at risk.

Improving IT asset management

Both the continuous monitoring[14] of information systems and incident response rely on strong IT asset management—understanding what assets the Department has and deploying strong endpoint protection for those assets. Properly managing these assets remains a challenge for the Department. In April 2022, we alerted Department leadership that the Office of the Secretary lacked effective endpoint protection capabilities.

Recent Office of Management and Budget (OMB) guidance[15] requires the Department to adopt robust endpoint detection and response (EDR) capabilities to contribute to centralized, government-wide visibility of devices. Although the Department has selected an EDR solution, it faces a long process to fully deploy and integrate EDR capabilities at each bureau. Further, once EDR is deployed, the Department will have to ensure that this new solution is operating effectively and contributing to better detection and understanding of threat activity.

Securely managing user accounts and permissions

Our recent work has also shown how the Department continues to struggle with the principle of least privilege—the concept that a user's account should only be granted the minimum system access and resources needed to perform the job. During our audit of NOAA's Active Directories, we identified user accounts with excessive privileges that could increase the risk of a successful compromise.[16] That same audit noted that many accounts were still active even though they had not been used within the last 60 days.[17] Removing or disabling unnecessary

---

[11] OIG-22-023-I.

[12] DOC OIG, February 3, 2022. *NOAA Inadequately Managed Its Active Directories That Support Critical Missions*, OIG-22-018-A. Washington, DC: DOC OIG.

[13] DHS CISA. *Security Tip (ST04-006)*, *Understanding Patches and Software Updates* [online]. https://www.cisa.gov/tips/st04-006 (accessed July 19, 2022).

[14] Information security continuous monitoring is the process of maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

[15] Office of Management and Budget, October 8, 2021. *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*, M-22-01. Washington, DC: OMB. Available online at https://www.whitehouse.gov/wp-content/uploads/2021/10/M-22-01.pdf (accessed July 19, 2022).

[16] OIG-22-018-A.

[17] *Ibid.*

accounts is one way to reduce an organization's attack surface[18] and the risk of system compromise. Previous Active Directory audits have identified similar issues at both USPTO[19] and the Census Bureau,[20] showing a pattern of problems related to identity or account management at the Department.

These findings continue a trend we noted in last year's *Top Management and Performance Challenges Facing the Department of Commerce* report (*Top Management Challenges*) report—poor account management, including granting user privileges beyond what is necessary. If the Department does not consistently follow the principle of least privilege and practice good account management, it cannot reduce the impact from cyberattacks.

Creating an effective risk management program

We have identified instances of security weaknesses stemming from the ineffective implementation of the National Institute of Standards and Technology (NIST) *Risk Management Framework* across multiple recent audits.[21] Such weaknesses suggest that the Department faces significant challenges in implementing a mature risk management program. Both federal requirements and Department policy set this *Risk Management Framework* as the standard for managing organizational risk and ensuring effective information security and privacy programs.

We examined the Department's system security assessment process, a crucial part of the framework, and found that the Department does not have a clear understanding of security control effectiveness across its bureaus.[22] In addition, we found that the Department's system security assessments were improperly planned and unreliable.[23] When the Department did identify issues, its remediation plans were not resolved in a timely manner.[24] This leads us to conclude that the Department makes risk-based security decisions using incomplete and inaccurate data.

Evidence has appeared in other audits as well. We identified certain NSS that had never received regular system assessments.[25] Additionally, our audit of the Department's cloud-based high value assets revealed that control documentation related to cloud security was

---

[18] 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 Computer Security Resource Center. *Attack surface (definition)* [online]. https://csrc.nist.gov/glossary/term/attack_surface (accessed July 25, 2022).

[19] 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.

[20] 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.

[21] *See* (1) DOC OIG, January 25, 2022. *The Department Needs to Improve Its System Security Assessment and Continuous Monitoring Program to Ensure Security Controls Are Consistently Implemented and Effective*, OIG-22-017-A. Washington, DC: DOC OIG; and (2) OIG-22-023-I.

[22] OIG-22-017-A.

[23] *Ibid.*

[24] *Ibid.*

[25] OIG-22-023-I.

incomplete.[26] Furthermore, our FY 2022 Federal Information Security Modernization Act (FISMA) audit identified that the Department did not have an 'effective' risk management function. These instances clearly demonstrated how the Department is struggling to maintain a baseline risk management program.

Finally, during a recent investigation into a cyberattack, we encountered a challenge pursuing remedies against the contractor. Specifically, the contracts did not sufficiently require the contractor to attest to the cybersecurity standards it claimed to have followed or to report a cyber-breach to the government upon discovery. While the compliance obligation rests with the contractors and grantees, government personnel—such as contracting officers, grants officers, and program officers—have a role in promoting this compliance and determining whether contractors and grantees are delivering the required level of cybersecurity, as specified in their contracts and grants. Where contractors and grantees fail to meet cybersecurity requirements, it is incumbent on Department staff to take prompt action to hold them accountable. Without specific contract and grant provisions in place, the government will be more limited in the types of remedies it can pursue against contractors and grantees that fail to effectively safeguard information systems. Any instances of fraud or reckless noncompliance with material cybersecurity requirements should immediately be referred to OIG, which may seek criminal and civil remedies through the U.S. Department of Justice.[27]

Adopting Revision 5 of the NIST Security and Privacy Controls standard[28]

Federal agencies are required to implement security and privacy controls specified in *NIST SP 800-53*. Revision 5 of this document was published in September 2020, and enterprise-wide compliance was expected by September 2021.[29] Among other significant modifications, revision 5 integrates privacy control requirements and adds many more controls and control enhancements,[30] including incorporation of three additional control families to the core catalog.[31] The Department is currently updating its security policy to reflect and define the new requirements, but the draft has not been finalized. As a result, the Department and its bureaus still face additional workload to implement required changes to IT security controls. Fully adopting revision 5 of *NIST SP 800-53* presents significant challenges that will require much effort at the enterprise, bureau, and system level to achieve compliance.

---

[26] DOC OIG, September 14, 2022. *Missing Security Controls Put the Department's Cloud-Based High Value Assets at Risk*, OIG-22-031-A. Washington, DC: DOC OIG.

[27] OIG is a partner in the U.S. Department of Justice's Civil Cyber-Fraud Initiative announced on October 6, 2021. This initiative seeks to use the False Claims Act to pursue civil actions against government contractors and grantees who fail to meet cybersecurity obligations.

[28] DOC NIST, September 2020. *Security and Privacy Controls for Information Systems and Organizations*, NIST SP 800-53, Revision 5 (updated December 2020). Gaithersburg, MD: DOC NIST. Available online at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (accessed July 26, 2022).

[29] OMB's *Circular No. A-130* expects federal agencies to meet the requirements of, and be in compliance with, NIST standards and guidelines within one year of their respective publication dates unless otherwise directed.

[30] Revision 5 adds 66 new controls and 202 new control enhancements.

[31] The three additional control families are supply chain risk management, personally identifiable information processing and transparency, and program management.

Transitioning to zero-trust architecture

The President's May 2021 executive order on zero-trust cybersecurity principles[32] marked a dramatic shift in the federal government's cybersecurity philosophy. The order established many new requirements and outlined an extensive path forward, with the intention of hardening federal government systems. It labels the prevention, detection, assessment, and remediation of cyber incidents as a top priority, essential to national and economic security.

Zero trust moves away from the longstanding perimeter-defense mindset and embraces a defense-in-depth strategy. Historically, organizations focused most of their effort on building robust protections around the network perimeter. Once users gained access and became insiders, they could roam freely on the network as trusted entities. The philosophy of zero trust is to remove implicit trust from an IT security strategy and to continuously validate interactions between users and resources on the network. Instead of giving full trust to insiders, zero trust allows for additional protection checkpoints each time a user wants to access data. Thus, even insiders will encounter more scrutiny.

In response to this paradigm shift, OMB released *Memorandum M-22-09* in January 2022.[33] Several other memos were also issued by OMB to pursue the goals of the order.[34] In conjunction, these memorandums provide executive agencies with detailed, actionable targets to timely implement a flurry of new requirements over the next several years.

Implementing zero trust will require comprehensive changes to the Department's IT security program. While some new requirement deadlines extend into 2024, the Department must continue to prioritize these changes throughout FY 2023 to meet the forthcoming deadlines. In fact, the Department failed to implement some requirements by the defined deadlines. For example, the Department did not meet the requirement to adopt MFA and data encryption agency-wide by November 8, 2021. The Department has submitted its plans to implement the requirement to OMB and the U.S. Department of Homeland Security, but the plans did not include a timeline for completion. New requirement challenges and deadlines stemming from the executive order and OMB memoranda are listed below.

---

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

[33] OMB, January 26, 2022. *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, M-22-09. Washington, DC: OMB. Available online at https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf (accessed July 26, 2022).

[34] *See* (1) OMB, August 10, 2021. P*rotecting Critical Software Through Enhanced Security Measures*, M-21-30. Washington DC: OMB. Available online at https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-30.pdf (accessed July 26, 2022); (2) OMB, August 27, 2021. *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, M-21-31. Washington, DC: OMB. Available online at https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf (accessed July 26, 2022); (3) OMB, M-22-01; and (4) White House, January 19, 2022. *Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems*, NSM-8. Washington, DC: White House. Available online at https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/ (accessed July 26, 2022).

In progress—not yet fully implemented

- Deploy and mature EDR solutions beginning February 2022.[35]
- Deploy MFA and encryption by November 2021.[36]
- Incorporate CISA's cybersecurity incident and vulnerability response playbooks (released in November 2021).[37]
- Adopt the NIST secure software development framework (effective March 2022).[38]

Due within one year

- Implement NIST guidance to protect critical software by August 2022.[39]
- Reach security event logging maturity level 1 by August 2022, level 2 maturity by February 2023, and level 3 maturity by August 2023.[40]

FY 2024 and beyond

- Fully implement zero-trust architecture by September 2024.[41]
- Continue to apply the requirements stemming from Executive Order 14028 to NSS.[42]

Many of the new requirements listed above touch on longstanding challenges facing the Department, as described in the *Continuing to Mature the IT Security Program* challenge. The Department must incorporate these new requirements as part of its efforts to modernize and mature its IT security program.

Progress made/challenges remaining since the FY 2022 TMC

During the previous FY, the Department and its bureaus made progress in addressing some of the challenges we identified in our FY 2022 *Top Management Challenges* report. For example, we have observed improvement in the incident response capabilities of the Enterprise Security Operations Center and the Census Bureau, with the Department closing our

[35] The Department has been working with CISA on this front. More guidance and requirements will be forthcoming.

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

[37] *See* DHS CISA, November 16, 2021. *New Federal Government Cybersecurity Incident and Vulnerability Response Playbooks.* Washington, DC: DHS CISA. Available online at https://www.cisa.gov/uscert/ncas/current-activity/2021/11/16/new-federal-government-cybersecurity-incident-and-vulnerability (accessed July 26, 2022). OMB guidance on agency use of the playbooks is forthcoming.

[38] White House, March 7, 2022. *OMB statement on "Enhancing the Security of Federally Procured Software*" [online]. https://www.whitehouse.gov/omb/briefing-room/2022/03/07/omb-statement-on-enhancing-the-security-of-federally-procured-software/ (accessed July 26, 2022).

[39] *See* OMB, M-21-30.

[40] *See* OMB, M-21-31.

[41] *See* OMB, M-22-09.

[42] White House, NSM-8. The National Manager for National Security Systems has begun issuing guidance and deadlines for implementing the new standards for NSS.

recommendations.[43] The Department also increased the maturity of two function areas related to FISMA from FY 2020 to FY 2021 and maintained this improvement in FY 2022.[44]

While the Department has recognized the importance of addressing IT security challenges in its strategic plan[45] and continues to make improvements, it must identify and mitigate the challenges affecting its ability to protect its IT systems. We believe that longstanding weaknesses will remain until the IT security program is consistently implemented across all the Department's bureaus. Maturing the overall IT security program and adopting zero-trust principles will be top Department challenges for the coming years.

[43] *See* 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.

[44] There are five FISMA function areas: *Identify*, *Protect*, *Detect*, *Respond*, and *Recover*. The Department increased its maturity for *Identify* and *Respond* from FY 2020 to FY 2021.

[45] DOC. *U.S. Department of Commerce Strategic Plan 2022 – 2026*. Washington, DC: DOC, Strategic Objective 1.6. Available online at https://www.commerce.gov/sites/default/files/2022-03/DOC-Strategic-Plan-2022%E2%80%932026.pdf (accessed July 26, 2022).

Challenge 2: Ensuring Continuity of Environmental Data from Satellites, Ships, Aircraft, and Ground-Based Systems and Improving Weather and Climate Services

NOAA's satellite systems, fleet of ships, and aircraft provide environmental data that are critical inputs to weather and climate forecasts provided by the National Weather Service (NWS), which also gathers data via ground-based systems such as radar. The National Environmental, Satellite, Data, and Information Service (NESDIS) is responsible for NOAA's satellites, and the Office of Marine and Aviation Operations (OMAO) is responsible for NOAA's fleet of ships and aircraft.

NESDIS continues deploying its Geostationary Operational Environmental Satellites (GOES)-R series, Joint Polar Satellite System (JPSS), and space weather satellites and is formulating programs for next-generation systems. OMAO is working to refresh its aging fleet of ships and aircraft.

OIG's FY 2023 top management and performance challenges include these priority areas related to NOAA programs:

- Maintaining continuity of geostationary and polar satellites
- Developing the next generation of satellite systems
- Protecting observations, operations, and communications from frequency interference
- Moving toward an operational collision avoidance support service
- Recapitalizing ships and aircraft
- Balancing weather service improvements and longer-term climate resilience

Maintaining continuity of geostationary and polar satellites

Delivering a fully capable GOES-U to support the geostationary satellite constellation[46]

A key performance challenge for NESDIS will be to build, test, and launch the fourth and last satellite in the GOES-R series, GOES-U (which will become GOES-19 on orbit), in 2024. In addition to the suite of Earth and space observing instruments flown on prior GOES-R series satellites, it will include a new space weather instrument. In FY 2023, the program will complete the bulk of satellite integration and testing, which must be well executed to ensure performance requirements can be met.

GOES-U represents the program's remaining opportunity to provide fully capable -East, -West, and on-orbit spare satellites until the follow-on geostationary program, Geostationary Extended Observations (GeoXO), begins launching in the early 2030s timeframe. GOES-17, which

[46] A system of satellites is also referred to as a *constellation.*

currently serves as the operational GOES-West[47] satellite, cannot fulfill all of the mission's key performance parameters due to degradation of its Advanced Baseline Imager.[48] It will be relegated to an on-orbit spare after GOES-18, which launched March 1, 2022, completes on-orbit testing and takes over the GOES-West operational role, currently planned for January 2023.

Launching JPSS-2 and managing development risks for JPSS-3 and -4 satellites

The JPSS program experienced challenges during integration and testing of the JPSS-2 satellite, which delayed the satellite's launch from September 2022 to November 2022. The program identified and mitigated some issues during JPSS-2's integration and testing and should capture these as lessons learned for the remaining missions. JPSS-3 and -4 satellite development projects are managing challenges stemming primarily from two key instruments. Further, JPSS-3 and -4 missions include plans to store the satellites before launch, a practice the program has not exercised with the preceding missions.[49]

Developing the next generation of satellite systems

While NOAA's current geostationary, polar, and space weather satellites will continue to provide key environmental observations for another decade, NOAA is currently investing in the next generation of these satellites to ensure long-term continuity. According to NOAA, it will seek to significantly improve data and products with its next-generation architecture. However, our work has identified weaknesses in requirements management that present risks to future satellite systems' architecture, design, and implementation efforts.[50]

In FY 2023, NESDIS plans to complete instrument formulation studies for its GeoXO program, which is the most mature of the next-generation programs and is a follow-on to the GOES-R series. During the formulation phase, NESDIS will define the program's plan and baseline its costs, schedule, and requirements. As part of this effort, it will be important for NESDIS to validate and prioritize GeoXO requirements—particularly those beyond the observations of the legacy GOES programs—before its first major procurement, planned for FY 2023.

NESDIS plans to replace its traditionally large polar satellites (such as JPSS) with smaller satellites (those with fewer instruments or only one instrument). Its QuickSounder mission will serve as a bridge between JPSS and the next generation of polar satellites. QuickSounder will

[47] NESDIS operates two satellites—known as GOES-West and GOES-East—to cover the operationally required geographic area and maintains one backup satellite in a storage orbit position to pick up the -East or -West mission if either one of the primary operational satellites fails. See DOC OIG, January 20, 2022. *Redesigned GOES-T is Ready for Launch, but NOAA Should Reassess Its Assumptions for Satellite Launch Planning and Storage*, OIG-22-015-A. Washington, DC: DOC OIG, p. 1.

[48] 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, p. 3–4.

[49] DOC OIG, July 9, 2018. *Polar Follow-On: NOAA Must Maintain Cost Efficiencies and Refine Launch Strategy for JPSS-3 and JPSS-4 Missions*, OIG-18-021-A. Washington, DC: DOC OIG, p. 4.

[50] DOC OIG, June 8, 2022. *The Success of NOAA's Next-Generation Satellite System Architecture Depends on Sound Requirements Management Practice*s, OIG-22-022-A. Washington, DC: DOC OIG.

host a spare Advanced Technology Microwave Sounder (one of the primary instruments on JPSS-era satellites). Along with QuickSounder, NOAA will need to concurrently pursue instrument development studies for a follow-on series of polar satellites. The challenge will be to create rapid procurement practices with timely infusion of new technology.[51]

NESDIS is also planning a Space Weather Next (SW Next) program whose first satellite would launch in FY 2028. The program is currently in an early planning phase and intends to start development in FY 2023. Its preliminary mission concept also includes partnering with other satellite programs to host space weather instruments. However, the program has been challenged in defining its mission concept through adequate partnerships. As one example, NESDIS determined that it could not accommodate SW Next instruments on GeoXO satellites in order for that program to maintain planned launch dates.

Protecting observations, operations, and communications from frequency interference

The Federal Communications Commission has yet to adopt lower international limits to power levels for a 5G cellular band adjacent to a key frequency remotely sensed by polar weather satellites. Even with lower power levels, these 5G transmissions may interfere with and potentially degrade the quality of those observations and, as a result, some weather forecasts. NOAA has informed Congress it needs additional resources to develop a strategy to mitigate the remaining impacts.

Additionally, NOAA and the National Telecommunications and Information Administration (NTIA) are exploring ways that a private company can use a frequency band adjacent to Global Positioning System and GOES Rebroadcast communications while minimizing interference. NOAA is also developing a "Radio Frequency Interference Monitoring System" that will monitor and detect probable interference in this frequency band.

NOAA's challenge continues to be to develop proactive, strategic plans to manage spectrum risk and ensure the success of its missions. NOAA needs adequate staff with spectrum knowledge to meet this challenge. However, it was not successful in securing funding for staff with spectrum-related experience in FY 2022. NOAA's FY 2023 budget again requests additional funding to increase staffing to inform decision making on spectrum-related issues.

Moving toward an operational collision avoidance support service

The Department still faces challenges in enhancing commercial space technologies and capabilities by providing a collision avoidance support service, as envisioned in *Space Policy Directive-3* (*SPD-3*).[52] Concern for avoiding collisions in space is growing, given the expected increase in orbiting satellites over the next several years.

NOAA's Office of Space Commerce (OSC) is responsible for developing space situational

[51] OIG-18-021-A, p. 9.

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

awareness and space traffic management capabilities. OSC had an acting director from January 2021 until a politically appointed director started in May 2022. OSC is hiring additional staff, including a deputy director. While its approved staffing level in FY 2022 was 20, OSC had only 4 employees as of June 2022. NOAA's FY 2023 budget justification requested an increase of 15 positions, for a total of 35.

NOAA also requested an increase of $77,700,000 for OSC (from FY 2022 funding of $10,000,000) to support developing space situational awareness capability for civil and commercial space sectors.[53] The additional funding will support NOAA's efforts to accelerate development from a pilot demonstration to an initial operating capability no later than FY 2024, with full operating capability in FY 2025. A substantial portion of the increase will be used to provide cloud services to host the capabilities and procure commercial data.

It is important that OSC quickly increase its staffing and efficiently use its increased funding (should it be appropriated) to successfully integrate various systems to develop these capabilities. Other challenges include (1) meeting *SPD-3* requirements to communicate space situational awareness information and (2) engaging domestic and international partners to use that information to manage their satellites and avoid collisions. In the second matter, there is no legal mechanism or authority to require operators to take actions based on the outputs of these capabilities.[54] To meet *SPD-3* requirements, the capabilities should include

- data integrity measures to ensure data accuracy and availability;
- data standards to ensure sufficient quality from diverse sources;
- measures to safeguard proprietary or sensitive data, including national security information;
- satellite owner-operator orbital location and planned maneuvers information; and
- standardized formats to enable development of applications to leverage the data.

Recapitalizing ships and aircraft

OMAO manages and operates a variety of specialized ships that play a critical role in the collection of oceanographic, atmospheric, hydrographic, and fisheries data. The current fleet of 15 ships was launched and commissioned between 1967 and 2014. The ships have an average age of 25 years, and more than half are currently operating beyond their originally designed service lives. By FY 2028, OMAO expects to decommission at least half of its ships as they reach the end of their useful service life.

To address the aging fleet, OMAO developed fleet recapitalization plans. OMAO is currently working from its 2016 plan, which should be adjusted for changing conditions and requirements to optimize the fleet's capability, performance, and affordability. The plan seeks to improve fleet readiness through annual appropriations of $75 million from FYs 2016–2028 for ship development and construction. We published a report recommending that OMAO develop and

[53] DOC National Oceanic and Atmospheric Administration, *Budget Estimates Fiscal Year 2023*, MS-101.

[54] *See* OIG-19-022-A, Other Matter.

regularly update a long-range plan to support program requirements.[55] However, while OMAO developed a draft 2020 fleet plan, it never finalized the document. According to NOAA, it is revising the draft plan, which will be routed to the Department and OMB for approval in FY 2023.

OMAO aircraft provide a wide range of specialized airborne environmental data collection capabilities vital to understanding the earth, conserving and managing coastal and marine resources, and protecting lives and property. According to NOAA, based on OMAO's aircraft service life expectation and historical usage analysis, its hurricane reconnaissance and research mission capabilities are at risk by 2030. OMAO is in the process of updating its 2019 recapitalization plan to extend and sustain aircraft capabilities.

OMAO efforts to procure new hurricane surveillance aircraft have been challenged with delays to modifications to a Gulfstream G550 that will postpone initial operating capability until September 2024 and necessitate the extended use of legacy aircraft. OMAO is also reporting a need for additional appropriations to complete these activities.

NOAA's ship and aircraft recapitalizations are complex, multi-year acquisitions that require effective planning, execution, and oversight to ensure maximum long-term benefit to the agency and the taxpayer. NOAA must manage challenges and risks in the acquisition, development, and construction of its fleet of ships and aircraft to avoid gaps and ensure continuity of mission operations.

Balancing weather service improvements and longer-term climate resilience

To reduce the impacts of climate change and severe weather events, the Department increased its emphasis on creating climate-resilient communities in its FY 2022–2026 strategic plan.[56] In our FY 2022 *Top Management Challenges* report,[57] we stated the Department must ensure its recent investments sustain improvements in cost-effective systems to meet the Weather Research and Forecasting Innovation Act of 2017[58] (2017 Weather Act) goal to improve forecasting of high-impact weather events such as tornadoes and hurricanes.

Tornadoes, which have caused more than twice as many deaths in the United States as hurricanes since 1940, are a continuing forecast challenge. From 2017–2021, forecast performance worsened, averaging nearly 8 minutes warning lead time compared with more than 13 minutes lead time during 2007–2011.[59] False alarm rates remain high, which can potentially erode trust in weather services and decrease the likelihood that people will take

[55] DOC OIG, May 25, 2021. *OMAO Must Define and Implement a Disciplined Requirements Management Process to Ensure Future Acquisitions Meet User Needs,* OIG-21-027-1. Washington, DC: DOC OIG, p. 2-7. *Note:* Our office contracted with The MITRE Corporation—an independent firm—to perform this evaluation.

[56] DOC, *Strategic Plan*.

[57] DOC OIG, October 14, 2021. *Top Management and Performance Challenges Facing the Department of Commerce in FY 2022*, OIG-22-001. Washington, DC: DOC OIG, p. 13-14.

[58] Pub. L. No. 115-25 (2017).

[59] Lead time is the elapsed time from warning issuance to event occurrence. The Department goal is 13 minutes.

protective actions.[60] Less frequent but with larger geographic impact, hurricanes contributed more than half of the $145 billion in weather-related damages in 2021.[61] However, NOAA has improved track and intensity forecast performance over time.[62] For both tornadoes and hurricanes, NWS initiated strategies to address improvements mandated by the 2017 Weather Act, including better specifying uncertainty and communicating risks.

In addition to the forecast challenge, a March 2022 tornado event in Iowa garnered media attention when a dissemination issue with weather service systems resulted in delays of up to 7 minutes communicating warnings following a network interruption. The event highlighted a previously unknown issue in the backup dissemination infrastructure, which forecasters had to mitigate as the severe weather occurred. As the event showed, trained forecasters are an important part of quality weather services—but NWS continues to have staffing and workforce structure challenges that have persisted for the last decade.

Ensuring national weather radar continuity and minimizing coverage gaps

The Next Generation Weather Radar (NEXRAD) program is the most important tool for issuing short-term, severe weather warnings. The NEXRAD system is undergoing a technological refresh to sustain the existing network coverage through at least 2035 as part of the Service Life Extension Program. The Department's follow-on system is not expected to be operational earlier than 2040, so refreshing the existing system while managing the replacement schedule will be important for maintaining critical radar coverage.

If the frequency of high-impact weather events increases due to a changing climate, a fully trained and robust workforce will be needed to forecast a larger number of individual severe weather events successfully and reduce their negative impacts on life and property. As NOAA attempts to improve communication of its services, forecasters need reliable systems to produce and disseminate their products before high-impact weather events so communities can act on them.

Progress made/challenges remaining since the FY 2022 TMC

Our FY 2022 *Top Management Challenges* report discussed aspects of most of these same challenges (with the exception of the "NOAA's Fleet Recapitalization Strategy" section). NOAA made progress and has challenges remaining in the following areas:

- The GOES-R program launched its GOES-T satellite (becoming GOES-18) on March 1, 2022, and is continuing through post-launch testing. GOES-U completed its integration and started environmental testing.
- The JPSS program completed environmental testing on the JPSS-2 spacecraft. Test

[60] A false alarm indicates a warning that was issued for an event that did not occur. Approximately 7 of every 10 tornado warnings in 2021 were false alarms.

[61] Hurricane Ida alone caused $78.7 billion in damages, the fifth costliest storm on record.

[62] See DOC NOAA. *National Hurricane Center Forecast Verification—Performance Measures and Goals* [online]. https://www.nhc.noaa.gov/verification/verify8.shtml (accessed July 25, 2022).

anomalies delayed satellite launch readiness from September 2022 to November 2022.

- NESDIS initiated the QuickSounder low earth orbit mission. The GeoXO program completed milestone 1 in November 2021 and is working towards milestone 2 approval in December 2022.
- NOAA was denied additional spectrum staffing in the FY 2022 budget but is again requesting the additional staff funding to better focus on spectrum-related issues.
- OSC initiated a pilot of its cloud-based space situational awareness repository that was tested against 20,000 space objects in collaboration with the U.S. Department of Defense, the National Aeronautics and Space Administration, and the commercial sector. A new politically appointed director started at OSC on May 9, 2022.
- Construction began on the Class A Ship *Oceanographer* in mid-FY 2022 and is expected for the ship *Discoverer* later in FY 2022. For Class B ships, the program issued the request for proposals in mid-FY 2022.
- NOAA secured funding for aircraft fleet recapitalization in FY 2022 that will allow OMAO to procure a third King Air aircraft and further support its development of the Gulfstream G550 hurricane surveillance aircraft. Additionally, Section 40006 of the Inflation Reduction Act of 2022, Pub. L. No. 117-169, provided $100 million for a second G550. However, according to NOAA, the program is currently projecting a shortfall of $24 million over FYs 2023–2025 needed to complete instrumentation and outfitting of both G550 aircraft.
- NWS operationalized new service backup capabilities for its River Forecast Centers through the National Water Center and multiple new forecast model versions that are intended to improve hurricane, heavy rainfall, and flood forecasts.

Challenge 3: Managing IT Investments and Improving Supported Operations

As the Department seeks to acquire two enterprise IT solutions, it must carefully manage complex challenges inherent to IT investments to ensure each new system will meet its cost, schedule, and performance goals. The U.S. Government Accountability Office (GAO) lists managing 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.[63]

OIG's FY 2023 top management and performance challenges for the Department include these priority areas related to IT investments:

- Avoiding further delays to Business Applications Solution (BAS) implementation
- Managing risks to the implementation of an enterprise grants management system

Avoiding further delays to BAS implementation

The BAS program is replacing the Department's legacy systems with commercial off-the-shelf applications to provide a new financial system for the Department. The BAS system will be an integrated suite of financial management, acquisitions management, and property management applications connected to a new enterprise data warehouse, business intelligence reporting platform, and data archiving solution. Given that BAS will replace outdated systems that enable the Department to plan and budget, award contracts and grants, and manage government property, this program is a critical step toward modernized mission support functions.

In support of this initiative, the Department awarded a 20-year contract to acquire the new applications, configure each to achieve required business outcomes, and deploy the applications at the Department's three finance bureaus.[64] BAS' original cost was $341 million, but has increased to $353 million due to a 1-year delay in system implementation announced in February 2022. Though the program conducted some implementation work from October 2021 through January 2022 in support of launching the new applications at NOAA by October 2022, the program delayed full implementation at NOAA until October 2023. The program also delayed implementation at NIST and the Census Bureau until October 2024 and October 2025, respectively. The program plans to use the additional time to accelerate delivery of some features and address escalating program risks and challenges that caused the delay.

[63] U.S. Government Accountability Office, March 2, 2021. *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, GAO-21-119SP. Washington, DC: GAO, p. 103.

[64] All Department bureaus are included within the scope of this modernization effort except for USPTO, which will only be included in the scope of BAS' enterprise data warehouse. NOAA's client bureaus are the Bureau of Industry and Security and the Economic Development Administration. NIST's clients are NTIA, Office of the Secretary, International Trade Administration, First Responder Network Authority, OIG, National Technical Information Service, Bureau of Economic Analysis, and Minority Business Development Agency. The Census Bureau does not support any clients.

As the Department implements BAS, the program must adequately reengineer business processes and manage organizational change—which includes managing requirements, updating its business process reengineering plan, capturing adequate risk information, optimizing new business processes, and using a consistent methodology to implement the new system.[65] In addition, the program has reported challenges in coordinating with other ongoing projects within the Department (e.g., the common grants management system), developing additional interconnection service agreements, implementing and testing security controls, working with limited resources, addressing training conflicts, and managing custom code modules.

Managing risks to the implementation of an enterprise grants management system

The Department continues working to replace three different grants management systems used by the bureaus with a common Grants Enterprise Management Solution (GEMS). However, the deployment of GEMS was delayed by 9 months due to BAS schedule delays because GEMS depends on an interface with the BAS financial management application. Currently, the GEMS program plans to transition NOAA to the new system by March 2024 and will transition NIST by March 2025.

In addition, GEMS implementation faces challenges in program management and systems integration. Specifically, in early 2022, the U.S. Economic Development Administration (EDA) opted to use alternative grants management software. NTIA will use this same software as a web-based portal for grant applications that interfaces with its current grants management system. The bureaus took these steps due to urgent needs in distributing funds associated with pandemic relief and broadband deployment.[66] EDA and NTIA shared concerns that the GEMS application would not be timely or flexible enough to meet their grant programs' needs. Neither has plans to exclusively use GEMS; instead, both plan to integrate their alternative application with GEMS at a later date.

The GEMS program's challenges from EDA's and NTIA's use of alternative software will require further analysis and updates to the migration plans, cost, and schedule. In addition, there is an ongoing Quality Service Management Office review of EDA's and NTIA's use of the alternative grant management application that could force the bureaus to abandon their alternative system plans and instead proceed with implementation of GEMS.[67]

The Department needs to carefully monitor GEMS risks—particularly BAS dependencies, EDA's and NTIA's use of alternative systems, and data migration risks[68]—that could continue to

---

[65] DOC OIG, July 7, 2022. *The BAS Program Needs to Increase Attention to Business Process Reengineering and Improve Program Management Practices*, OIG-22-025-A. Washington, DC: DOC OIG.

[66] *Coronavirus Aid, Relief, and Security Act*, Pub. L. No. 116-136 (2020); *American Rescue Plan Act of 2021*, Pub. L. No. 117-2 (2021); *Consolidated Appropriations Act, 2021*, Pub. L. No. 116-260 (2020); and *Infrastructure Investment and Jobs Act*, Pub. L. No. 117-58 (2021).

[67] OMB designated the U.S. Department of Health and Human Services to run a Quality Service Management Office with responsibility for offering and managing a marketplace of grants systems and service solutions across the federal government.

[68] OIG-22-001, p. 19.

affect GEMS' cost, schedule, and performance. Given these potential risks to program success, the Department will also be challenged to ensure the GEMS application provides the capability to effectively manage all its grant programs.

Progress made/challenges remaining since the FY 2022 TMC

The Department made progress on this previously reported[69] challenge:

- BAS concluded its design phases (global design and common solution) in October 2021.
- BAS conducted pilot demonstrations of the new software with NOAA and other key stakeholders to continue addressing business process reengineering and organizational change management challenges.

However, the Department continues to face challenges in areas we previously identified:

- In a July 2022 report on the BAS program, we identified the need for improvements in business process reengineering, requirements management, and risk management.[70]
- The GEMS program continues to track risks related to the migration of legacy grants data and the further degradation of legacy grants systems.

[69] *Ibid*, p. 18–19.

[70] OIG-22-025-A.

Challenge 4: Ensuring Prudent Financial Management and Oversight of Broadband Infrastructure Funding

The Department faces a new challenge in conducting effective oversight of broadband infrastructure funding. The COVID-19 pandemic has underscored the critical importance of affordable, high-speed broadband for individuals, families, and communities to be able to work, learn, and connect remotely. Increasing access to broadband is an ongoing national challenge.

OIG's FY 2023 top management and performance challenges include these priority areas related to NTIA's broadband infrastructure program:

- Acquiring and maintaining sufficient staff with proficiency to ensure proper oversight and use of funds
- Implementing the appropriate measures to prevent, detect, and report potential fraud and hold grantees, subgrantees, contractors, and subcontractors accountable for performance

Acquiring and maintaining sufficient staff with proficiency to ensure proper oversight and use of funds

In 2021, President Biden signed the Infrastructure Investment and Jobs Act (IIJA),[71] which appropriated roughly $65 billion to ensure that every American has access to reliable high-speed internet. The IIJA included a historic investment in broadband infrastructure deployment that builds on investments from previous laws, including the American Rescue Plan Act (ARPA) and the Consolidated Appropriations Act, 2021 (CAA). As a result of receiving an additional $48 billion in funding for broadband infrastructure, NTIA will implement the following new programs:

- The Broadband Equity, Access, and Deployment Program provides $42.45 billion—to be distributed among all 50 states, the District of Columbia, and certain U.S. territories—for projects that support broadband infrastructure deployment and adoption.
- IIJA appropriates $1 billion to NTIA to create the Enabling Middle Mile Broadband Infrastructure Program. The purpose of this grant program is to expand and extend middle mile infrastructure to reduce the cost of connecting unserved and underserved areas to the internet backbone.
- IIJA provides an additional $2 billion to the existing Tribal Broadband Connectivity Program, an NTIA program previously implemented under CAA. This program directs funding to tribal governments for broadband deployment on tribal lands, as well as for telehealth, distance learning, broadband affordability, and digital inclusion.
- The Digital Equity Act Programs will distribute $2.75 billion to promote digital inclusion and equity, ensuring that all individuals and communities can acquire the necessary skills, technology, and capacity to engage in the nation's digital economy.

[71] Pub. L. No. 117-58 (2021).

This significant increase in funding and deployment of these new programs will place additional demands on NTIA's existing workforce, oversight processes, business practices, and financial management systems to ensure proper oversight and use of the funds. Shortages of experienced staff with the right skills and abilities can contribute to delays in the deployment of these new programs. NTIA will need to quickly organize existing staff and hire additional temporary staff to meet the objectives of the IIJA.

Further, since 2011, we have reported that the Department continues to face challenges regarding its acquisition and grants workforce. For example, we stated in last year's *Top Management Challenges* report[72] that the Department continues to face workforce challenges such as its inability to (1) attract and retain experienced professionals to work in locations outside the Washington, DC, metropolitan area and (2) fill vacant positions timely. The Department needs to ensure NTIA can provide sufficient oversight with limited time and staff, especially with the significant increase in broadband infrastructure funding.

In response to these challenges, we plan to initiate two audits of NTIA: (1) to evaluate NTIA's ability to acquire and maintain sufficient staff with proficiency to ensure prudent financial management and oversight over the use of broadband infrastructure funds, and (2) to determine whether NTIA is adequately monitoring grants awarded under CAA.

Implementing appropriate measures to prevent, detect, and report potential fraud and hold grantees, subgrantees, contractors, and subcontractors accountable for performance

NTIA will need to adequately specify in each of its contracts and grants all material qualifications, requirements, and performance goals and ensure they flow down to any subgrantees and subcontractors. Each contract and grant should also include provisions allowing NTIA to recover funds in the event of noncompliance. While the compliance obligation rests with the awardees and subawardees, government personnel—such as program officers, grants officers, and contracting officers—should communicate to all awardees and subawardees the importance of (1) complying with contract and grant requirements, (2) preventing and detecting fraud or noncompliance, and (3) reporting any suspected fraud or reckless noncompliance to NTIA and OIG.

Throughout the life cycle of the awards—from the application to the closeout phase—NTIA should require awardees and subawardees to provide reports and other information related to material qualifications, requirements, and performance goals, and formally attest to the accuracy and completeness of each submission. Without such attestations, it can be difficult to pursue certain remedies and ultimately hold awardees and subawardees accountable. NTIA will need to ensure that (1) each awardee and subawardee submission receives sufficient review and (2) any deficiencies are promptly resolved. Any instances of suspected fraud or reckless noncompliance with contract or grant requirements should be immediately referred to OIG, which may investigate further and seek criminal and civil remedies through the U.S. Department of Justice. To facilitate these potential remedies, NTIA should ensure that all contract- and

[72] OIG-22-001.

grant-related information, including all information and reports submitted by the awardees and subawardees, is readily accessible.

Challenge 5: Enforcing Fair and Secure Trade and Effectively Implementing Export Controls

Among the federal government's leading trade enforcement and promotion agencies, the Department faces the 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 Department 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.

Realigning U.S.-China trade relations to counter China's unfair and anticompetitive policies and create a level playing field for U.S. companies is a key goal of President Biden's 2022 Trade Policy Agenda.[73] Under the direction of the Chinese Communist Party, China's military-civil fusion (MCF) strategy seeks to acquire foreign technology through both licit and illicit means for China's military modernization. Similarly, U.S. trade relations with Russia also are a focus of the administration. In response to Russia's invasion of Ukraine, BIS imposed strict export controls on Russia, including on a range of items subject to the Export Administration Regulations (EAR) that did not previously require export licenses when destined for Russia.

OIG's FY 2023 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
- Combating China's MCF strategy
- Ensuring proper implementation of export controls related to Russia's invasion of Ukraine

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

The Department's ability to combat trade barriers continues to be an ongoing challenge. We have noted trade barriers as a challenge in last year's *Top Management Challenges* report. In the Department's *FY 2022–2026 Strategic Plan*, one of the Department's strategic goals addresses policies or actions by foreign governments that impede the exports of U.S. goods and services.

Furthermore, as previously reported in last year's *Top Management Challenges* report, 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

[73] Office of the United States Trade Representative, Executive Office of the President, March 2022. *2022 Trade Policy Agenda and 2021 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/2022%20Trade%20Policy%20Agenda%20and%202021%20Annual%20Report%20(1).pdf (accessed June 10, 2022).

is proactively identifying, monitoring, and resolving trade barriers to ensure American businesses and workers can compete on an even playing field within foreign markets.[74] The Secretary stated that to fulfill this goal, ITA will defend U.S. workers by addressing unfair foreign trade practices and barriers, strengthening enforcement of U.S. trade laws, and enhancing oversight of foreign government compliance with trade agreements.[75]

Combating China's MCF strategy

China's MCF program seeks to leverage technological advancements in strategic industries for military development. This strategy is designed to develop the most technologically advanced military in the world by 2049 through the elimination of barriers between China's civilian research and commercial sectors and its military and defense industrial sectors. The targeted technologies include quantum information sciences, robotics, semiconductors, aerospace technologies, biotechnology, and artificial intelligence, many of which have "dual-use" (military and civilian) applications. China uses imports, foreign investments, commercial joint ventures, mergers and acquisitions, and industrial and technical espionage to help achieve its military modernization goals.

BIS' two business units—Export Administration and Export Enforcement—each play a role in combating MCF. Export Administration (1) publishes rules to impede China's acquisition of sensitive U.S. technologies that it could use to develop weapons, military aircraft, or surveillance technology; (2) places controls on emerging technologies; (3) identifies and adds to the Entity List[76] foreign parties that are prohibited from receiving some or all items subject to the EAR without a license from BIS; and (4) processes export licenses.[77] Export Enforcement (1) investigates unauthorized exports that can result in criminal and administrative penalties; (2) reviews export license applications; and (3) recommends persons and entities for the Entity List, Denied Person Lists, Military End-User List,[78] and Unverified List.

---

[74] 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/FA546C8A-80A0-4AA8-8F78-D13D137DE06D (accessed August 15, 2022).

[75] 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 August 12, 2022).

[76] The EAR contain a list of names of certain foreign persons—including businesses, research institutions, government and private organizations, individuals, and other types of legal persons—that are subject to specific license requirements for the export, reexport, or in-country transfer of specified items. These persons comprise the Entity List, which is found in Supplement No. 4 to Part 744 of the EAR. On an individual basis, the persons on the Entity List are subject to licensing requirements and policies supplemental to those found elsewhere in the EAR.

[77] BIS uses its Commerce USXPORTS Exporter Support System to process export licenses and support export enforcement and technical licensing determination functions.

[78] The Military End-User List (Supplement No. 7 to part 744 of the EAR) identifies foreign parties that are prohibited from receiving items described in Supplement No. 2 of Part 744 of the EAR unless the exporter secures a license. The U.S. government determined these parties to be 'military end users,' as defined in Section 44.21(g) of

BIS stated in its *FY 2023 Budget Request* that it is strengthening efforts to address strategic national security threats, including attempts by countries of national security concern such as China and Russia, to obtain U.S. items to improve military capabilities. BIS' workload is increasing and BIS reported that since 2019, the number of BIS enforcement cases opened involving China has increased by 79 percent. Similarly, the volume of overall export license applications processed increased almost 20 percent and the volume of license determinations for enforcement action increased by approximately 40 percent over the same period. To address this challenge, BIS will need to prioritize its workload and ensure adequate staffing is in place to investigate enforcement cases and identify persons and entities that are violating published rules when sending U.S. technology to China.

Ensuring proper implementation of export controls related to Russia's invasion of Ukraine

BIS administers and enforces the 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.[79] 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 export controls that BIS imposed on Russia in the wake of its invasion of Ukraine include highly restrictive license requirements on all categories of items exported to Russia and Belarus that are on the Commerce Control List (CCL).[80] These actions expand U.S. scrutiny of transactions to almost any sensitive dual-use technology, software, or commodities that Russia could use to support its war effort. As a matter of policy, BIS denies applications involving these items, many of which were not previously subject to controls when destined for Russia. These measures specifically impose new CCL-based license requirements for Russia, add new Foreign Direct Product rules[81] specific to Russia and Russian military end users, significantly restrict the use of EAR license exceptions,[82] and expand the existing Russia 'military end use' and 'military end user' control scope to all items subject to the EAR. As of June 2, 2022, BIS also added 322 entities to the Entity List for acquiring and attempting to acquire items subject to the EAR in support of Belarus's and/or Russia's militaries or military modernization efforts. The ability to

---

the EAR, who represent an unacceptable risk of use in or diversion to a 'military end use' or 'military end user' in China, Russia, or Venezuela.

[79] Pub. L. No. 115-232 (2018). 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.

[80] The CCL is a list of categories and product groups used to help determine whether U.S. exports need an export license from the Department.

[81] Foreign-produced items located outside the United States are subject to the EAR when they are a direct product of specified technology or software, or are produced by a plant or major component of a plant that itself is a direct product of specified technology or software.

[82] A license exception is an authorization that allows the export or reexport, under stated conditions, of (1) items subject to the EAR that would otherwise require a license under General Prohibition One, Two, Three, or Eight as indicated under one or more of the Export Control Classification Numbers in the CCL in Supplement No. 1 to part 774 of the EAR and (2) items subject to the EAR that would require a license based on the embargo policies described in part 746 of the EAR.

enforce these new controls depends on the appropriate monitoring of license requirements and identification of end users and end use. End-use checks (EUCs) consist of physically verifying the parties to the transaction to determine the reliability of the recipient and ensure that the recipient will use U.S. goods in accordance with EAR. As part of its licensing regimen, BIS conducts selective EUCs on exports of dual-use goods and various military items to monitor license compliance. Also, BIS must enforce these new controls in addition to managing an increased export licensing workload due primarily to the transfer of jurisdiction of thousands of items from the U.S. Munitions List to the CCL as part of the Export Control Reform Initiative.[83] Given the large increase in the number of items subject to export controls, BIS must enhance its monitoring efforts to ensure compliance. In 2020, we found that that BIS needs to improve its efforts to effectively track and monitor EUC performance to ensure the appropriate foreign end users receive and use controlled U.S. exports in accordance with the EAR.[84]

Progress made/challenges remaining since the FY 2022 TMC

In our FY 2022 *Top Management Challenges* report, we highlighted as a priority area "combating unfair trade practices by effectively resolving trade barriers and enforcing U.S. trade agreements."[85] We are currently conducting an audit of ITA's efforts to resolve foreign trade barriers.[86] Our objective is to assess the progress and actions taken by ITA to remove, reduce, and prevent foreign trade barriers.

[83] 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 August 12, 2022).

[84] See DOC OIG, March 2, 2020. *Lack of Defined Processes and Procedures Impede Efforts to Monitor End-Use Check Performance*, OIG-20-019-A. Washington, DC: DOC OIG.

[85] OIG-22-001, p. 22.

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

Challenge 6: Deploying a Nationwide Public Safety Broadband Network

The Middle Class Tax Relief and Job Creation Act of 2012 (the Act) established the First Responder Network Authority (FirstNet Authority) as an independent authority within NTIA to ensure the building, deployment, and operation of a National Public Safety Broadband Network (NPSBN) dedicated to first responders.[87] On March 28, 2017, FirstNet Authority entered into a 25-year indefinite-delivery, indefinite-quantity contract with AT&T for the construction and operation of the NPSBN. FirstNet Authority's arrangement with AT&T involves (a) an initial obligation of up to $6.5 billion in funds to AT&T to deploy the NPSBN, (b) AT&T's use of dedicated broadband spectrum, and (c) spectrum lease payments from AT&T to FirstNet Authority over the life of the contract, which supports FirstNet Authority's operations and improvements to the NPSBN.

OIG's FY 2023 top management and performance challenges for the Department, NTIA, and FirstNet Authority include the following priority areas related to FirstNet Authority:

- Ensuring a sound reinvestment process
- Ensuring appropriate task order oversight
- Ensuring proper NPSBN adoption and coverage

We previously identified these topics in our FY 2022 *Top Management Challenges* report.[88] Our subsequent audit and ongoing work relate to FirstNet Authority's reinvestment process and contract oversight.[89]

Ensuring a sound reinvestment process

The NPSBN contract requires AT&T to make required annual fixed payments to FirstNet Authority over 25 years totaling $18 billion, of which approximately $15 billion is expected to be used for reinvestments to maintain and improve the network. FirstNet Authority received its first payment in April 2018 and, to date, has received six payments[90] totaling $795 million. Due to the significant amount of reinvestment funds, it is crucial that FirstNet Authority's reinvestment decision-making process is sound (i.e., transparent, logical, and justified) and helps FirstNet Authority to select investment opportunities that will best support the evolving mission and risk-based needs of public safety[91] prior to approval of new investments.

---

[87] *Middle Class Tax Relief and Job Creation Act of 2012*, Pub. L. No. 112-96 §§ 6204(a), 6206(b) (2012).

[88] *See* OIG-22-001, p. 36–37.

[89] *See* DOC OIG, August 25, 2022. *FirstNet Authority Did Not Have Reliable Cost Estimates to Ensure It Awarded Two Reinvestment Task Orders at Fair and Reasonable Prices*, OIG-22-029-A. Washington DC: DOC OIG; and DOC OIG, September 9, 2020. *Audit of FirstNet Authority's Reinvestment Process*, #2020-381. Washington, DC: DOC OIG.

[90] Per the NPSBN contract, with the exception of the first payment, the payments are due 2 weeks before the start of the subsequent FY.

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

The FirstNet Authority reinvestment process is used to identify, analyze, and select investments to maintain, operate, and improve the NPSBN. In FY 2022, we identified significant issues with FirstNet Authority's reinvestment process in (1) an audit focused on the process FirstNet Authority used for developing Independent Government Cost Estimates (IGCEs) for its initial two investments[92] and (2) an ongoing audit on the process used to develop and select the initial investments.

IGCEs

In our August 25, 2022, report,[93] we found that FirstNet Authority did not follow GAO's *Cost Estimating and Assessment Guide* when preparing and documenting IGCEs used to evaluate its first two reinvestment proposals. Specifically, we found that FirstNet Authority did not (1) sufficiently document IGCEs, (2) ensure that IGCEs reflected updates based on changed conditions, (3) justify fair and reasonable pricing for additional requirements proposed by AT&T that were not included in the IGCEs, (4) address legal review concerns, and (5) develop a cost estimating plan describing the steps for preparing an IGCE. Further, we found that FirstNet Authority accepted, without providing sufficient justification, AT&T's price proposals for both investments that exceeded the IGCEs by 60 percent or more. FirstNet Authority needs to take several actions to better prepare IGCEs in the future to ensure costs are reasonable and fair.[94] We received concurrences from the Department and NTIA[95] that will ensure actions are taken to address the deficiencies we found.

Generation of investment ideas

Our ongoing audit of FirstNet Authority's reinvestment process[96] is assessing if FirstNet Authority has established a sound process for identifying and selecting reinvestment opportunities. Without a sound business process for generating and selecting its initial two investments, FirstNet Authority may not be able to demonstrate that the investment opportunities were the most appropriate and/or efficient use of resources[97] for (1) reducing performance gaps of the network and/or (2) meeting first responders' priorities of evolving

[92] The initial two investments consisted of expanding deployable capabilities and Phase 1 of the 5G upgrade.

[93] OIG-22-029-A.

[94] *Ibid*, p. 9–10.

[95] *Ibid*, p. 19–23.

[96] DOC OIG, #2020-381.

[97] The *DOC Scalable Acquisition Project Management Guidebook* "provides the information needed by Department and Bureau project managers to conduct cost-effective and efficient acquisitions by implementing the *Scalable Acquisition Project Management Framework*." The *Guidebook* states that the *Framework* depicts the lifecycle of a project that "begins with the identification of mission requirements to support strategic goals and objectives, proceeds with the determination of the best solution for meeting those requirements, and then directs the acquisition of that solution in the most appropriate, efficient, and effective way." Finally, the *Guidebook* states, "[i]n essence, first 'determining the right thing to do,' and then 'doing it the right way.'" DOC, August 31, 2015. *DOC Scalable Acquisition Project Management Guidebook*, version 1.2. Washington, DC: DOC, p. 5-6.

operational needs.[98] A sound reinvestment process is essential to ensure future reinvestments of billions of dollars are supported and justified and reflect public safety priorities.[99]

Ensuring appropriate task order oversight

Ensuring appropriate task order oversight is one of FirstNet Authority's FY 2023 top management challenges. As we noted in our FY 2022 *Top Management Challenges* report, we previously identified persistent issues with FirstNet Authority's contract oversight.[100] Our ongoing audit of FirstNet Authority's contract oversight[101] is assessing if FirstNet Authority has adequately evaluated contractor performance for its initial two reinvestments. Conducting sufficient contractor oversight is essential to ensure the government receives what it purchases and that the needs of public safety officials are addressed.

Ensuring proper NPSBN adoption and coverage

While our recent audit efforts focused on the reinvestment task orders, additional risks surrounding key objectives within the NPSBN contract remain. We initiated two audits in the second half of FY 2022 to evaluate FirstNet Authority's oversight of the NPSBN coverage and device connection targets.[102] FirstNet Authority is responsible for determining whether AT&T is meeting the nationwide coverage and device connection targets. We noted in our FY 2022 *Top Management Challenges* report that our review of metrics identifying device connections by state illustrated that AT&T was previously at risk of not meeting state-specific device connection targets.[103] As the NPSBN is intended to be a nationwide network, FirstNet Authority needs to closely monitor and oversee contract performance with respect to verifying coverage claims and the state-by-state device connection totals to meet the Act's intent of a nationwide network and public safety adoption of the NPSBN. There is a risk to public safety if coverage is not implemented in the agreed-upon areas within the agreed-upon timeframes.

Additionally, appropriate oversight is imperative to monitor the execution of the NPSBN contract. At predetermined milestones, the NPSBN contract requires FirstNet Authority to pay AT&T incentive payments for meeting coverage and device connection targets, and AT&T is required to pay FirstNet Authority disincentive payments if the device connection targets are

[98] We expect to issue this report in the first quarter of FY 2023.

[99] It was publicly reported that the 2020 FirstNet Authority Roadmap, which was developed and utilized by FirstNet Authority, is tied to its resource allocation process and ensures investments in the network are fully aligned with the specific needs of the public safety community. *See* FirstNet Authority. *First Responder Network Authority Roadmap*. Reston, VA: FirstNet Authority. Available online at https://www.firstnet.gov/system/tdf/Roadmap_2020_nocompress.pdf?file=1&type=node&id=1612&force= (accessed September 13, 2022).

[100] OIG-22-001, p. 43.

[101] DOC OIG, #2020-381.

[102] Connection targets are used to measure the number of device connections and verify public safety's adoption of the network.

[103] OIG-22-001, p. 38.

not met. As these milestones are tied to payments, oversight of these objectives is imperative to ensure that FirstNet Authority is paying only for services provided.

Progress made/challenges remaining since the FY 2022 TMC

FirstNet Authority continues to report on progress made implementing the NPSBN. At its May 4, 2022, board meeting,[104] the Board approved a resolution that provides Agency Deployed Radio Access Network capability to primary subscribing agencies. The FirstNet Board reported that this investment to provide a small cell product that operates on the Band 14 spectrum will improve the NPSBN experience for public safety, provide reliable FirstNet connection, and bring mission-critical services indoors, such as PushToTalk and video.

Additionally, at its August 17, 2022, board meeting,[105] FirstNet Authority reported that (1) the NPSBN was being used by more than 21,800 public safety agencies via more than 3.7 million device connections; (2) the NPSBN maintained an inventory of more than 150 dedicated deployable network assets; (3) more than 200 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 95 percent).

[104] FirstNet Authority, May 4, 2022. *Combined Board and Committees Meeting.* Reston, VA: FirstNet Authority. Available online at https://www.firstnet.gov/sites/default/files/May_2022_Combined_Board_and_Committee_Meeting_Presentation_0.pdf (accessed on July 28, 2022).

[105] FirstNet Authority, August 17, 2022. *Combined Board and Committees Meeting.* Los Angeles, CA: FirstNet Authority. Available online at https://www.firstnet.gov/sites/default/files/August%202022%20Combined%20Board%20and%20Committees%20Meeting.pdf (accessed on September 12, 2022).

Challenge 7: Improving Management and Oversight of Contracts and Grants to Ensure Responsible Spending

A continuing challenge for the federal government, and the Department specifically, is ensuring that it spends taxpayer dollars prudently and safeguards programs from fraud, waste, and abuse. The Department faces ongoing challenges with proper contract and grant oversight and management. In FY 2021, the Department obligated more than $6.6 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 $2.9 billion in grants and other financial assistance awards. As of the third quarter of FY 2022, the Department has obligated more than $1.5 billion in grant and financial assistance awards in response to the COVID-19 pandemic.

It is paramount that the Department place sustained focus on its contract and grant awards and oversight to ensure that (1) recipients spend these funds efficiently and effectively and (2) the awards result in the expected quality of services, products, and performance. Our previous and ongoing work has identified several areas where the Department can better manage and oversee grants and contracts to improve program performance; achieve cost savings; and help prevent fraud, waste, and abuse.

OIG's FY 2023 top management and performance challenges for the Department include these priority areas related to acquisitions and grants:

- Ensuring the integrity of grant programs
- Ensuring programs approved for State Small Business Credit Initiative (SSBCI) funding comply with program requirements
- Developing and retaining a competent acquisition workforce to support the Department's mission

Ensuring the integrity of grant programs

Administering grant programs requires that the Department implement internal controls to ensure that it meets program goals and uses funds appropriately. For grant programs, this includes providing oversight and guidance to award recipients, as well as ensuring that grantees and subgrantees have the appropriate certifications for requirements that are material to grant award decisions. In FYs 2020 and 2021, the Department received more than $6.9 billion under the Coronavirus Aid, Relief, and Economic Security Act (CARES Act),[106] CAA,[107] and ARPA[108] to support the Department's response to the COVID-19 pandemic.[109] The significant increase

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

[107] Pub. L. No. 116-260, 134 Stat. 1182 (2020).

[108] Pub. L. No. 117-2, 135 Stat. 4 (2021).

[109] The CARES Act allocated funds to EDA, NTIA, NOAA, NIST, and the Minority Business Development Agency to assist communities affected by and responding to the COVID-19 pandemic.

in pandemic funds represents a considerable addition to normal grant administration, and oversight responsibilities will remain a challenge in the months and years to come.

One of the challenges the Department faces in ensuring adequate oversight of financial assistance is obtaining adequate staff to handle the demand of performing oversight of pandemic relief funds. We previously recommended that EDA develop and implement a comprehensive workforce plan to determine optimal staffing levels needed and identify potential staffing shortfalls or gaps.[110] EDA developed the workforce plan and has taken proactive steps to address this challenge by actively recruiting and hiring talent under a special hiring authority to meet the CARES Act requirements.

The total dollar amount of the Department's obligated grant awards has increased substantially in recent years after Congress passed multiple spending bills allocating funding for pandemic relief. For example, EDA's obligated grant award amounts doubled from $760 million in FY 2019 to $1.5 billion in FY 2021. Therefore, to continue ensuring that it properly and timely uses these funds, EDA must (1) ensure that the workforce plan is fully implemented and (2) recruit and maintain a highly skilled workforce as it increases its oversight of pandemic relief funds.

Ensuring programs approved for SSBCI funding comply with program requirements

ARPA reauthorized and amended the State Small Business Credit Initiative Act of 2010 to provide $10 billion to fund the SSBCI. This federal program, administered by the U.S. Department of the Treasury (Treasury), expands access to capital, promotes economic resiliency, creates new jobs, and increases economic opportunity. In April 2022, Treasury announced that the Minority Business Development Agency (MBDA) would receive $100 million in grant funding, which will focus its technical assistance on helping underserved entrepreneurs seeking direct capital investment.

Treasury OIG has indicated that "Treasury will face challenges in holding participants accountable for the proper use of funds, as Treasury has not clearly defined the oversight obligations of the states, U.S. territories, and tribal governments, or specified minimum standards to determine whether participants fulfilled their oversight responsibilities."[111] We also see this to be a challenge for the Department. We previously found that MBDA missed opportunities to resolve noncompliance with award requirements for other programs.[112] We reported that MBDA did not use all tools available to improve its oversight over financial assistance awards, program staff was inconsistent in monitoring recipients, and MBDA did not

[110] 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.

[111] U.S. Department of the Treasury Office of Inspector General, October 14, 2021. *Management and Performance Challenges Facing the Department of the Treasury*, OIG-CA-22-002. Washington, DC: Treasury OIG.

[112] DOC OIG, September 5, 2017. *MBDA Can Improve Processes to More Effectively Monitor Cooperative Agreements*, OIG-17-029-A. Washington, DC: DOC OIG.

always follow up when it found specific deficiencies.[113] Lack of controls or not using the controls in place increases the risk of improperly awarding grant funds or other grant compliance issues. Department management should have adequate controls in place to ensure that the Department successfully distributes and oversees grant funds and program integrity.

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

The Department's ability to hire and retain experienced staff is an ongoing challenge. Acquisition services require well-qualified 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 2021, the Department saw a 9.3 percent increase (from 331 to 362) in the number of acquisition professionals in the GS-1102 (Contracting) job series. In addition, the attrition rate decreased by approximately 5.9 percent (from 34 to 32).

During FY 2021, the Department has continued to address this issue of managing and strengthening its acquisition workforce. The Department established an acquisition innovation lab to facilitate the use of innovative and underutilized acquisition techniques and smart program management tools throughout the acquisition and program lifecycle. Additionally, the Department offered acquisition-related training classes through external and internal training to fulfill the Federal Acquisition Certification in Contracting requirements. 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 through the use of the Pathways Program and special hiring authorities to attract and retain highly qualified employees to meet hiring projections for a staff of 376 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:

- difficulty in attracting and retaining experienced acquisition professionals to work in and outside the Washington, DC, metropolitan area
- timeliness of filling vacancies
- scarcity of talent to procure and manage the Department's variety of highly specialized products and services due to federal government pay and incentives that are not competitive with the private sector
- other factors including continued budget cuts, a legislative hiring cap, lack of relocation funding incentives for highly qualified candidates, and limited career development and advancement opportunities.

[113] *Ibid.*

Progress made/challenges remaining since the FY 2022 TMC

The Department and its bureaus have made some progress on our previously reported FY 2022 top management and performance challenges. Our work in FY 2022 found significant weaknesses in Enterprise Services' (ES') management and oversight of the Accenture blanket purchase agreement.[114] Specifically, we found that (1) ES was not effective in enforcing performance requirements to ensure contract quality and timeliness standards were met and did not timely assess or adequately document contractor performance in the contractor performance assessment reporting system and (2) ES contracting officers and the assigned contracting officer's representatives did not properly maintain invoices or supporting documentation to demonstrate that invoices were reviewed and work was performed prior to approving invoices for payment. ES has since developed and implemented procedures to enforce contractual requirements, developed and implemented an issue tracking system, and incorporated bureau/order level performance data in formal performance assessments under the recompeted contract.

The Department continues to face challenges in several areas that we previously identified. In April 2022, Department employees began returning to the office. However, some employees continue to work remotely and within hybrid work environments (such as periodic telework mixed with in-office work). In these remote and hybrid work environments, the Department must maintain its capability to administer and manage contract and grant files electronically for multiple contractors and grantees. Our ongoing[115] and prior audit work[116] continues to identify significant vulnerabilities in how the Department manages contract and grant file documentation, which could expose the Department to substantial financial losses. The Department's increase in funding due to the pandemic, combined with employees working remotely and in a hybrid environment, may continue to present additional challenges to the Department's efforts to manage and retain contract and grant files.

[114] DOC OIG, November 22, 2021. *Enterprise Services Needs to Improve Upon Its Contract Management and Oversight of Accenture BPA No. DOCSS130116BU0004 and Subsequent Call Orders*, OIG-22-009-A. Washington, DC: DOC OIG.

[115] DOC OIG, October 16, 2020. *Evaluation of EDA's Grant File Maintenance*, #2021-385. Washington, DC: DOC OIG.

[116] *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; (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; and (3) DOC OIG, December 21, 2020. *EDA Is Not Fully Complying with All Its Disaster Relief Award Policies*, OIG-21-014-A. Washington, DC: DOC OIG.

Challenge 8: Establishing a Strong Framework with Adequate Resources to Support the 2030 Census Planning Efforts and Enhance Overall Survey Quality

Fiscal year 2023 marks the last FY of the 2020 Census funding lifecycle and the second one for the 2030 Census lifecycle. As the Census Bureau stated in its FY 2023 Congressional budget justification, this period of transition when it can learn from the previous decennial census to inform plans for the next one "is a once-in-a-decade opportunity to further refine the Census Bureau's stewardship of the American people's mission, data, and taxpayer dollars for decades to come."[117] For FY 2023, the Census Bureau is requesting funding to continue its program of research and testing centered on developing a 2030 Census design. This design will capitalize on several innovations, such as the way the address list is developed and maintained, the use of administrative records as a source of data for enumeration, and making field operations more efficient.

Looking ahead, the Census Bureau must continue its evaluation of 2020 Census successes and identify areas for improvement for the next decennial census. Also, the Census Bureau should continue initiatives to maintain the quality of surveys that it carries out.

OIG's FY 2023 top management and performance challenges include these priority areas related to the Census Bureau:

- Ensuring the timely delivery of 2020 Census studies and the timely completion of the *2020 Post-Census Group Quarters Review* needed to inform 2030 Census planning
- Ensuring information from the *Post-Enumeration Survey* (*PES*) is used to develop a strategy for obtaining a more accurate count of certain demographic groups and state populations for the 2030 Census
- Enhancing the accuracy and reliability of the Census Bureau's address list
- Ensuring data products provide timely, reliable, and quality data to stakeholders

Ensuring the timely delivery of 2020 Census studies and the timely completion of the 2020 Post-Census Group Quarters Review *needed to inform 2030 Census planning*

The 2020 Census Evaluations and Experiments (EAE) operation comprises three major types of studies designed to evaluate decennial census programs and operations: (1) assessments that contain operational metrics (such as workloads and costs) that document how the Census Bureau conducted 2020 Census operations, like the nonresponse followup (NRFU) field operation; (2) evaluations that analyze, interpret, and synthesize the effectiveness of census components and their impact on data quality, coverage, or both; and (3) experiments that identify possible designs for early 2030 Census lifecycle research and testing. Additionally, the

[117] DOC Economics and Statistics Administration, March 2022. *U.S. Census Bureau's Budget Fiscal Year 2023*. Washington, DC: DOC ESA, CEN-3.

Census Bureau plans to provide reports on the results of quality control activities for several operations and issue a report on COVID-19's impact on the decennial census. For the 2020 Census, the Census Bureau plans to complete 46 assessments, 13 evaluations, 3 experiments, 3 quality control results reports, and 1 topic report through mid-FY 2025.[118] The timely completion of these studies and documentation of the results are key factors in being able to use the information for early 2030 Census planning. After the 2010 Census, we reported[119] that research delays with the studies[120] and a lack of budget integration threatened the 2020 Census design. Also, we found the practices of moving project baselines and postponing deadlines were the result of insufficient project planning and Census Bureau management's failure to confirm when stakeholders needed the studies' results for 2020 Census planning. Therefore, completing the EAE operation on time will be critical to helping the Census Bureau make well-informed 2030 Census design decisions.

In addition to EAE, the Census Bureau initiated a new, one-time operation for governmental units in the United States and Puerto Rico to request that the Census Bureau review the population counts of group quarters they believe were not correctly counted as of April 1, 2020. The operation was created in response to public feedback received on the Count Question Resolution operation about counting group quarters populations during the unprecedented challenges posed by the COVID-19 pandemic. The Census Bureau initiated the operation in May 2022 to improve the count of group quarters populations throughout the country. Expected to be completed on a rolling basis up through September 30, 2023, the *2020 Post-Census Group Quarters Review* affords the approximately 40,000 tribal, state, and local governments nationwide the opportunity to request a review of the count of their group quarters populations that they believe to be incorrect. Although the results of these reviews will not change the overall population counts from the 2020 Census that were used to apportion the number of seats in the U.S. House of Representatives, governmental units can incorporate updated group quarters population figures into the Population Estimates Program.[121] For programs that are funded on a per capita basis, these updates could increase funding for governmental units. Therefore, it is essential that the Census Bureau provide accurate and timely population updates through this program to revise future population estimates.

To assess the Census Bureau's progress in completing and documenting the results of the EAE studies, we initiated an evaluation to determine whether the Census Bureau adequately prepared EAE operational assessments and included the appropriate metrics needed to inform planning for 2030 Census research and testing.

[118] U.S. Census Bureau. *2020 Census Evaluations and Experiments (EAE)* [online]. www.census.gov/programs-surveys/decennial-census/decade/2020/planning-management/evaluate/eae.html (accessed September 16, 2022).

[119] DOC OIG, December 3, 2013. *2020 Census Planning: Research Delays and Program Management Challenges Threaten Design Innovation*, OIG-14-003-A. Washington, DC: DOC OIG.

[120] For the 2010 Census, this operation was called the Census Program for Evaluations and Experiments.

[121] The updated population base will be used by surveys, such as the American Community Survey, that contribute to providing communities with current information on social, economic, housing and demographic topics that help determine how federal and state funds are distributed.

Ensuring information from the PES is used to develop a strategy for obtaining a more accurate count of certain demographic groups and state populations for the 2030 Census

The *PES* is an interrelated set of operational activities intended to allow the Census Bureau to evaluate coverage of the 2020 Census and provide data to improve future decennial censuses. The Census Bureau conducts the *PES* to measure the coverage of housing units and people residing within them during the 2020 Census. The first release of *PES* data on March 10, 2022, reported that, overall, the percentage of persons counted for the 2020 Census was consistent with that of recent decennial censuses. However, based on data from the *PES*, the Census Bureau estimated significant undercounts of many of the same demographic groups, such as African Americans and Latinos, that have historically been undercounted. Some groups, such as non-Hispanic Whites and Asians, had estimated overcounts in the 2020 Census. On May 19, 2022, the Census Bureau released the 2020 Census undercount and overcount rates for the 50 states and the District of Columbia, which found that 6 states had population undercounts and 8 had overcounts.[122] If the *PES* results are accurate, it will be critical for the Census Bureau to use this information to develop a strategy to address undercounts and overcounts during 2030 Census planning.

In FY 2023, we will conduct an audit to assess the validity of the *PES* results as they relate to overcount and undercount of selected states.

Enhancing the accuracy and reliability of the Census Bureau's address list

The Census Bureau's master address file (MAF) is a national address list of housing units, group quarters, transitory locations, and some nonresidential addresses. It includes over 200 million address records, each one of which is linked to a referencing system to determine its location on a map. The MAF serves as the source of address and location information for the decennial census, *American Community Survey* (*ACS*), and other demographic surveys. It is updated using information from the U.S. Postal Service; tribal, state, and local governments; and other Census Bureau data collection operations. For prior decennial censuses, the Census Bureau conducted 100 percent in-field address canvassing to confirm the accuracy of the addresses in the MAF extract prior to enumeration. However, due in part to the cost of sending listers[123] to validate every housing unit in the United States, the Census Bureau developed an operation to reduce the number of housing units requiring an in-field visit.

Beginning in September 2015, the Census Bureau implemented a new operation called In-Office Address Canvassing to identify housing unit changes nationwide based on a review of satellite imagery. This operation was expected to reduce the in-field address canvassing workload to approximately 30 percent of all housing units as of May 2018. However, by September 2018, approximately 47 percent of housing units were found to require in-field verification. To reduce

[122] Population overcounts and undercounts are denoted by net coverage errors measured in percentages that are significantly greater than or less than zero, respectively.

[123] A lister was a Census Bureau employee who canvassed geographic blocks of addresses to validate potential living quarters.

the workload to approximately 41 percent, and thus the cost of the in-field address canvassing operation, the Census Bureau changed the criteria for identifying blocks requiring in-field address canvassing. As a result, not all housing units initially identified through in-office address canvassing were validated in the field.

Given the MAF's importance to both decennial and recurring survey operations, the Census Bureau should evaluate the completeness and accuracy of the MAF and the operations used to update it. If housing units are missing from or not accurately reflected in the MAF, they will not be selected for survey samples or invited to respond to the 2030 Census.

In FY 2023, we will assess the information obtained through the Local Update of Census Addresses operation to accurately update the MAF.

Ensuring data products provide timely, reliable, and quality data to stakeholders

The Census Bureau carries out demographic surveys for itself and for sponsors via interagency agreements to produce a wide range of statistics about the U.S. population. Through such an arrangement, a sponsor pays the Census Bureau to carry out its survey given the latter's vast experience and capabilities in this field. Representatives working in six regions throughout the country visit households to obtain information about people wherever they live—be it a house, apartment, mobile home, or group housing. Data from internal surveys, such as the *ACS* and the *Survey of Income and Program Participation*, provide information to stakeholders on demographic and housing data, consumer expenditures, income, health insurance data, and participation in government assistance programs. Data from sponsored surveys, such as the *Consumer Expenditure Survey* and the *Current Population Survey*,[124] provide information used to compile critical statistics such as the *Consumer Price Index* (which measures inflation) and monthly unemployment and labor participation rates.

However, data collected from these surveys are only as good as the sampling frame used to select households and the ability of field representatives to collect data accurately and according to procedures. This became evident in September 2019 when, following the release of 2017 *ACS* data products, the Census Bureau announced it had identified errors in the data for one county in Delaware, which impacted estimates for that county and the state overall. The errors occurred during personal interviewing data collection. For stakeholders and the public to have confidence in its data products, the Census Bureau must refine its processes to ensure data collected from households included in surveys are accurately recorded and produce information that meets users' needs.

We began an audit during FY 2022[125] to determine whether reimbursable surveys provide quality and reliable data to help sponsoring federal agencies make informed decisions.

[124] Both surveys are sponsored in whole or in part by the U.S. Department of Labor's Bureau of Labor Statistics.

[125] DOC OIG, January 14, 2022. *Audit of the U.S. Census Bureau Demographic Programs Directorate's Reimbursable Survey Data Quality and Reliability*, #2022-419. Washington, DC: DOC OIG.

Progress made/challenges remaining since the FY 2022 TMC

Ensuring data collection is high quality

Throughout FY 2022, we carried out work to assess data quality of both decennial and nondecennial census activities. On September 14, 2022, we issued a final report on lessons learned during the NRFU operation for the 2020 Census.[126] The report included the following challenges facing the Census Bureau as it plans for the 2030 Decennial Census: college students were likely undercounted at off-campus addresses; a significant number of enumerations were completed using a proxy; and improper execution of the NRFU quality assurance plan may have adversely affected data quality. In addition, we continued with fieldwork on our current audit of the Census Bureau's efforts to ensure data quality for its reimbursable surveys.[127]

Ensuring paid advertising efforts increased self-response to the 2020 Census

We initiated an audit of the 2020 Census integrated communications contract.[128] Our objective is to determine whether the Census Bureau effectively managed selected contract task orders related to paid advertising for the 2020 Census to ensure desired outcomes were achieved.

Ensuring only candidates suitable for federal government employment are hired

Our evaluation of the Census Bureau's employee background check process[129] found that the Census Bureau continued to face significant backlogs in adjudicating post-employment cases, lacked appropriate documentation and oversight of cases, did not adjudicate some pre-employment cases, and had incomplete data in its employment check system. We issued five recommendations aimed at addressing these deficiencies; the Census Bureau concurred with all of them and has begun taking actions to address them.

[126] DOC OIG, September 14, 2022. *Lessons Learned from the 2020 Decennial Census*, OIG-22-030. Washington, DC: DOC OIG.

[127] DOC OIG, #2022-419.

[128] DOC OIG, March 31, 2022. *Audit of the 2020 Census Paid Advertising Campaign*, #2022-423. Washington, DC: DOC OIG.

[129] DOC OIG, May 9, 2022. *The Census Bureau Needs to Improve Management and Oversight of Vetting Employees to Avoid Hiring Unsuitable Individuals for Federal Employment*, OIG-22-021-I. Washington, DC: DOC OIG.

Challenge 9: Strengthening U.S. Leadership in Intellectual Property

The United States' intellectual property (IP) system can quickly drive innovation to meet society's challenges. The COVID-19 pandemic response is an example, with government and private companies collaborating to discover, approve, and mass produce vaccines in record time—under 12 months. The products and technologies essential to COVID-19 vaccines resulted from pre-existing innovation made possible because of IP rights. IP rights provide incentives for companies and individuals to develop and commercialize inventions. It is critical that USPTO continue to conduct high-quality, timely patent and trademark examinations to drive innovation and maintain U.S. leadership in IP.

OIG's FY 2023 top management and performance challenges include these priority areas related to USPTO:

- Continuing efforts to improve and maintain patent quality and service
- Protecting and supporting registration processes and trademark owners
- Improving critical mission support functions

Continuing efforts to improve and maintain patent quality and service

USPTO continues to face challenges in providing quality patent decisions in an efficient and timely manner. USPTO patent operations have focused on the dual goals of decreasing examination time and increasing patent quality. As noted in our FY 2022 *Top Management Challenges* report, USPTO uses patent term adjustment (PTA) deadlines as its benchmark for timeliness.[130] The percentage of applications meeting the first office action benchmark (i.e., a first action on the merits[131] within14 months from application filing) has steadily declined. For example, USPTO met 42 percent of its first action PTA deadlines in February 2021, but by April 2022, it met 32 percent of first action PTA deadlines. In addition, the average length of first-action pendency rose in April 2022 to 19.4 months, an increase of more than 3 months from February 2021. With the examiner attrition rate rising to more than 4 percent in FY 2021, USPTO faces a substantial challenge to meet its timeliness goals.

USPTO has made improvements toward its self-measured quality standards. Nevertheless, improving quality and customer perception remains a challenge. In our FY 2022 *Top Management Challenges* report, we noted that USPTO fell short of its goal by 10 percentage points in its internal assessment of the correctness of obviousness rejections.[132] For the entirety

[130] 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* OIG-22-001, p. 31.

[131] An office action on the merits commonly cites prior art (references or documents which may be used to determine novelty and/or non-obviousness of claimed subject matter in a patent application) 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.

[132] OIG-22-001, p. 32.

of FY 2021, the Office of Patent Quality Assurance (OPQA) reported over 90 percent of obviousness assessments complied with law. While those numbers indicate substantial improvement, they also remain below USPTO's goal for 93 percent compliance, and indicate that approximately 1 in 10 assessments does not comply with law. Further, OPQA found only 81 percent of surveyed office actions were compliant under all statutes governing patentability (e.g., novelty, obviousness, subject matter and description), a level well below USPTO's goals for compliance with individual statutes. From its semiannual external quality survey, taken in the third quarter of FY 2021, USPTO reported that between 50 and 65 percent of respondents (depending on technology group) considered obviousness rejections to be correct "most of the time" or "all of the time." Continued efforts to improve quality—as measured both within USPTO and among external stakeholders—remain a challenge for USPTO.

Following the Supreme Court's *Arthrex* decision,[133] USPTO's Director may review final Patent Trial and Appeal Board (PTAB) decisions in *inter partes* review and post-grant review proceedings. The recently appointed Director is assessing USPTO's interim review process, with a focus on transparency and consistency. For example, the Director has published suggestions for particular information in requests for review and particular issues that may warrant Director review. However, these interim procedures are likely to be changed or augmented further, as USPTO intends to (1) seek comments from stakeholders concerning Director review and (2) formalize the review process. Management will be challenged to find processes that meet stakeholders' expectations, provide transparency in USPTO's work, and do not impede or delay effective decision making.

Protecting and supporting registration processes and trademark owners

USPTO has faced considerable growth in demand for trademark registration in recent years. Despite initial concerns about a drop in applications and revenues early in the COVID-19 pandemic, USPTO received record numbers of filings in both FY 2020 and FY 2021. The increase in FY 2021 alone was 27.9 percent. While filings have since fallen somewhat, USPTO still projected that FY 2022 filings would exceed FY 2020 levels. As a result, USPTO's backlog of pending applications awaiting an initial examination has grown to over 550,000, a more than 185 percent increase from 2 years ago. Trademark first action pendency[134] exceeds 7 months, more than double the historical levels prior to FY 2021. In recognition of the challenges, USPTO has reset its pendency goals and does not expect the goals to return to historical target levels until FY 2027. These longer wait times can burden businesses, forcing them to change brand strategies and leaving them uncertain about their trademark rights.

USPTO also continues to face concerns about fraudulent or inaccurate applications, which we have identified as a challenge in recent years. USPTO continues to introduce new initiatives to prevent and detect fraudulent or inaccurate applications, including in response to our FY 2021

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

[134] First action pendency measures the average number of months from the date of application filing to the examining attorney's first office action. The first office action provides an early indication of the issues that need to be addressed in order for the examining attorney to approve the application.

audit report on this topic.[135] These include suspending trademark practitioners who have acted improperly, using automated tools to verify information in applications, and upgrading access controls on trademark systems. However, USPTO continues to receive suspicious specimens of use and will face challenges from bad actors as they adapt their tactics to USPTO's controls.

Together, these challenges may put stress on USPTO's trademark workforce. The growing backlog and the need to identify increasingly sophisticated fraudulent applications threaten the morale of trademark staff. This could result in increased attrition at a time when USPTO is trying to grow its examining corps. USPTO plans to hire 100 new examining attorneys in FY 2023—increasing the examining corps by 9 percent from FY 2021. USPTO will need to train and supervise these additional examining attorneys while maintaining examination quality.

Improving critical mission support functions

Critical technical and administrative functions underpin USPTO's ability to carry out its mission. However, USPTO's IT investment and development are misaligned with budget planning and lack key performance indicators that are vital to support its effective review and processing of patents. USPTO also continues to face challenges related to the management and oversight of its foundational contracts.

In our recent audit of USPTO's patent legacy systems,[136] we found that USPTO's product teams should plan and prioritize IT capabilities into future years to determine the annual budget. USPTO created its Patent Product Line annual budget estimates without preparing a life-cycle cost estimate. We made recommendations for USPTO to follow Agile-related best practices to establish cost estimates that are based on an entire life cycle. We also found that USPTO needed to improve its Agile software development practices to deliver business value. To do this, we recommended that USPTO take action to ensure product team members develop comprehensive key performance indicators for each product. Our work continues to identify challenges for USPTO to develop next-generation systems to replace aging systems.

We previously reported that USPTO needed to improve its contract award processes and manage its contracts to ensure that contractors are performing adequately and that costs are validated and controlled.[137] In our recent audit of USPTO's Patent Data Capture (PaDaCap) contracts,[138] we found that USPTO needed to strengthen its procurement procedures to prevent unnecessary or unreasonable costs. Notably, USPTO incurred questioned costs of approximately $22.4 million that could have been prevented through earlier recompetition. In addition, USPTO's PaDaCap contractor regularly delayed cybersecurity updates and failed to provide adequate physical security. Given the critical function of the contract to manage the entire life cycle of patent application processing, it is imperative that USPTO mitigate risks to

[135] 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.

[136] OIG-22-026-A, p. 3.

[137] OIG-22-001, p. 35.

[138] DOC OIG, August 16, 2022. *USPTO Should Strengthen Its Planning and Oversight of Patent Data Capture Contracts to Manage Risks and Prevent Unnecessary Costs*, OIG-22-028-A, p. 6.

procurement oversight, hold contractors accountable, and ensure the prompt remediation of security risks.

Progress made/challenges remaining since the FY 2022 TMC

In last year's *Top Management Challenges* report, we noted the challenges for USPTO to (1) develop procedures for the Director's discretionary review of PTAB decisions and (2) address court challenges relating to the review process.[139] USPTO has published interim policies and processes for Director review but faces challenges in revising and formalizing them. Further, the Court of Appeals for the Federal Circuit decided whether reviews by the Commissioner for Patents (performing the duties of the Director pending nomination and confirmation of a Director) could stand. The court held that the Commissioner was authorized to perform the reviews when performing the functions and duties of the Director on a temporary basis[140] and denied a petition to rehear the appeal. It is unknown whether any party will petition the Supreme Court to hear the case—but for now, uncertainty over reviews performed before the new Director took office has been relieved.

USPTO finalized the regulations for the Trademark Modernization Act (TMA) within statutory timeframes and has begun accepting and processing filings under the TMA. While the number of filings has been modest so far, USPTO will need to devote appropriate resources to processing them as it addresses its backlog of applications.

[139] OIG-22-001, p. 33.

[140] *Arthrex Inc. v. Smith & Nephew, Inc.*, 35 F.4th 1328 (Fed. Cir. 2022).

Appendix A: Related OIG Publications

This list presents OIG's FY 2022 work related to top management and performance challenges facing the Department in FY 2023. 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 Effectiveness Through Zero Trust

- *The Department Needs to Improve Its System Security Assessment and Continuous Monitoring Program to Ensure Security Controls Are Consistently Implemented and Effective* (OIG-22-017-A; January 25, 2022)
- *NOAA Inadequately Managed Its Active Directories That Support Critical Missions* (OIG-22-018-A; February 3, 2022)
- *The Department Mismanaged, Neglected, and Wasted Money on the Implementation of IT Security Requirements for Its National Security Systems* (OIG-22-023-I; June 15, 2022)
- *Missing Security Controls Put the Department's Cloud-Based High Value Assets at Risk* (OIG-22-031-A; September 14, 2022)

Challenge 2: Ensuring Continuity of Environmental Data from Satellites, Ships, Aircraft, and Ground-Based Systems and Improving Weather and Climate Services

- *Redesigned GOES-T is Ready for Launch, but NOAA Should Reassess Its Assumptions for Satellite Launch Planning and Storage* (OIG-22-015-A; January 20, 2022)
- *The Success of NOAA's Next-Generation Satellite System Architecture Depends on Sound Requirements Management Practices* (OIG-22-022-A; June 8, 2022)
- *The Department Needs to Improve Its Metadata Processes Under the Geospatial Data Act* (OIG-22-032-A; September 22, 2022)

Challenge 3: Managing IT Investments and Improving Supported Operations

- *The BAS Program Needs to Increase Attention to Business Process Reengineering and Improve Program Management Practices* (OIG-22-025-A; July 7, 2022)

Challenge 4: Ensuring Prudent Financial Management and Oversight of Broadband Infrastructure Funding

Challenge 5: Enforcing Fair and Secure Trade and Effectively Implementing Export Controls

Challenge 6: Deploying a Nationwide Public Safety Broadband Network

- *FirstNet Authority Must Increase Governance and Oversight to Ensure NPSBN Security* (OIG-22-011-I; December 14, 2021)
- *FirstNet Authority Did Not Have Reliable Cost Estimates to Ensure It Awarded Two Reinvestment Task Orders at Fair and Reasonable Prices* (OIG-22-029-A; August 25, 2022)

Challenge 7: Improving Management and Oversight of Contracts and Grants to Ensure Responsible Spending

- *Audit of the Department's Digital Accountability and Transparency Act of 2014 Submission for the First Quarter of Fiscal Year 2021* (OIG-22-003-A; November 8, 2021)
- *WPRFMC's Governance of Western Pacific Sustainable Fisheries Fund Awards Was Inadequate* (OIG-22-004-A; November 10, 2021)
- *Inspector General Letter to Chairwoman Eddie Bernice Johnson re: Department Employees on Non-Reimbursable Details* (OIG-22-008-M1; November 17, 2021)
- *Inspector General Letter to Senators Hirono, Whitehouse, Blumenthal, Markey, and Warren re: Department Employees on Non-Reimbursable Details* (OIG-22-008-M2; November 17, 2021)
- *Enterprise Services Needs to Improve Upon Its Contract Management and Oversight of Accenture BPA No. DOCSS130116BU0004 and Subsequent Call Orders* (OIG-22-009-A; November 22, 2021)
- *The Department Must Improve Processes for Addressing and Managing 'H' Referrals* (OIG-22-014-I; December 16, 2021)
- *2022 Annual Letter to OMB re: Government Charge Card Abuse Prevention Act of 2012* (OIG-22-016-M; January 21, 2022)
- *IG Response Letter to Senator Thune re: NTIA TBCP* (September 2, 2022)
- *Performance Audit of the U.S. Department of Commerce's Working Capital Funds* (OIG-22-033-A; September 22, 2022)

Challenge 8: Establishing a Strong Framework with Adequate Resources to Support the 2030 Census Planning Efforts and Enhance Overall Survey Quality

- *The Census Bureau Needs to Improve Management and Oversight of Vetting Employees to Avoid Hiring Unsuitable Individuals for Federal Employment* (OIG-22-021-I; May 9, 2022)
- *Lessons Learned from the 2020 Decennial Census* (OIG-22-030; September 14, 2022)

Challenge 9: Strengthening U.S. Leadership in Intellectual Property

- *USPTO Has Opportunities to Improve Its Patent Examination Process and to Advance Patent Decision-Making* (OIG-22-010-I; December 2, 2021)
- *USPTO Needs to Improve Its Cost Estimating, Scheduling, and Agile Practices to Timely Retire Patent Legacy Systems* (OIG-22-026-A; July 20, 2022)
- *USPTO Should Strengthen Its Planning and Oversight of Patent Data Capture Contracts to Manage Risks and Prevent Unnecessary Costs* (OIG-22-028-A; August 16, 2022)

Appendix B: Acronyms and Abbreviations

2017 Weather Act	Weather Research and Forecasting Innovation Act of 2017
ACS	American Community Survey
Act	Middle Class Tax Relief and Job Creation Act of 2012
ARPA	American Rescue Plan Act
BAS	Business Applications Solution
BIS	Bureau of Industry and Security
CAA	Consolidated Appropriations Act, 2021
CARES Act	Coronavirus Aid, Relief, and Economic Security Act
CCL	Commerce Control List
Census Bureau	U.S. Census Bureau
CISA	Cybersecurity & Infrastructure Security Agency
Department	U.S. Department of Commerce
Director	Under Secretary of Commerce for Intellectual Property and Director of USPTO
EAE	Evaluations and Experiments
EAR	Export Administration Regulations
EDA	U.S. Economic Development Administration
EDR	Endpoint detection and response
EOL	End of life
ES	Enterprise Services (Department)
EUC	End-use checks
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 Solution
GeoXO	Geostationary Extended Observations
GOES	Geostationary Operational Environmental Satellites
IGCE	Independent Government Cost Estimate
IIJA	Infrastructure Investment and Jobs Act
IP	Intellectual property

IT	Information technology
ITA	International Trade Administration
JPSS	Joint Polar Satellite System
MAF	Master address file
MBDA	Minority Business Development Agency
MCF	Military-civil fusion
MFA	Multifactor authentication
NESDIS	National Environmental Satellite, Data, and Information Service
NEXRAD	Next Generation Weather Radar
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
NPSBN	National Public Safety Broadband Network
NRFU	Nonresponse followup
NSS	National Security Systems
NTIA	National Telecommunications and Information Administration
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
PaDaCap	Patent Data Capture
PES	Post-Enumeration Survey
PTA	Patent term adjustment
PTAB	Patent Trial and Appeal Board
SSBCI	State Small Business Credit Initiative
SW Next	Space Weather Next
TMA	Trademark Modernization Act of 2020
TMC	Top Management Challenges
Treasury	U.S. Department of the Treasury
U.S.	United States
USPTO	United States Patent and Trademark Office

011200000425