Top Management and Performance Challenges Facing the Department of Commerce in Fiscal Year 2024

U.S. Department of Commerce
Office of Inspector General

Report No. OIG-24-002
October 12, 2023

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 12, 2023

CC: Don Graves, Deputy Secretary of Commerce
Eric Morrissette, Chief of Staff
André Mendes, Chief Information Officer
Jeremy Pelter, Deputy Assistant Secretary for Administration, performing the non-exclusive functions and duties of the 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 2024***
Final Report No. OIG-24-002

The Office of Inspector General is required by statute[1] to annually report the most serious management and performance challenges facing the U.S. Department of Commerce. Attached is our final report on the Department's top management and performance challenges for fiscal year 2024. The report includes detailed discussions of the issues listed below.

Challenge 1: Continuing the transition to zero trust to overcome IT security shortcomings and strengthen cybersecurity

- Continuing the transition to zero trust
- Improving IT security shortcomings and strengthening cybersecurity

Challenge 2: Awarding and overseeing grants to expand broadband access to all Americans

- Ensuring funding is properly allocated and awarded to close the digital divide
- Overseeing broadband programs with challenging regulatory and National Telecommunications and Information Administration requirements
- Optimizing workforce to manage increases in grant administration activities
- Implementing measures to prevent, detect, and report potential fraud and hold grantees and subgrantees accountable for performance

[1] 31 U.S.C. § 3516(d).

Challenge 3: Promoting growth in domestic semiconductor manufacturing and research

- Hiring and retaining qualified staff in a competitive labor market
- Implementing adequate internal controls and oversight

Challenge 4: Enhancing weather, water, and climate services

- Maintaining a robust satellite architecture
- Ensuring successful ship replacement efforts and communicating impacts of a potential gap in high-altitude aircraft observations
- Increasing the National Weather Service's effectiveness at protecting life and property in a changing climate

Challenge 5: Leveraging trustworthy artificial intelligence and modernizing IT systems

- Leveraging trustworthy artificial intelligence to ensure safe and effective enhancements of operations and services
- Modernizing IT systems

Challenge 6: Effectively enforcing export controls and supporting U.S. supply chain resilience

- Ensuring effective enforcement of export controls to counter China's Military-Civilian Fusion strategy
- Ensuring effective enforcement of export controls on Russia and Belarus
- Promoting U.S. supply chain resiliency through timely and impactful analysis
- Combating unfair trade practices by effectively resolving trade barriers and enforcing U.S. trade agreements

Challenge 7: Ensuring public safety entities have the network services they need to respond effectively to emergencies

- Ensuring FirstNet Authority's appropriate oversight of the Nationwide Public Safety Broadband Network (NPSBN) contract's task orders
- Ensuring AT&T is meeting its goals for NPSBN adoption and coverage
- Ensuring only eligible users have access to the NPSBN
- Ensuring FirstNet Authority's innovation and test lab benefits public safety entities

Challenge 8: Managing and overseeing contracts and grants while ensuring equitable procurement

- Managing contract and grant awards, oversight, and program performance
- Managing, strengthening, and retaining a skilled acquisition workforce to support the Department's mission
- Ensuring equity in procurement

Challenge 9: Safeguarding intellectual property to promote innovation and economic prosperity

- Adapting to emerging technologies
- Maintaining the integrity of the patent application system and trademark register
- Improving patent and trademark quality and timeliness
- Improving critical mission support functions

Challenge 10: Ensuring the Census Bureau provides quality data to stakeholders

- Incorporating lessons learned from the 2020 group quarters count into 2030 census planning
- Ensuring survey operations help produce reliable and accurate population estimates

Challenge 11: Protecting funds awarded under the Public Wireless Supply Chain Innovation Fund grant program

- Implementing strong internal controls to meet timelines and ensure funds are properly awarded

Challenge 12: Ensuring strong oversight and effective use of funding for National Institute of Standards and Technology construction and maintenance

- Prioritizing complex construction and maintenance projects
- Ensuring prudent financial management and oversight of funds

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.

We appreciate the cooperation we have 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 about this report, please contact me at (202) 793-3336.

[2] *Ibid*.

Contents

Cover graphics from Adobe Stock (stock.adobe.com)
Front cover background by cameraman
Back cover background by bridgman

Challenge 1: Continuing the transition to zero trust to overcome IT security shortcomings and strengthen cybersecurity

In June 2023, Chinese hackers breached the email accounts of multiple high-level Department of Commerce officials, including the Secretary of Commerce. This successful hacking attempt underscored the cruel reality that securing the Department's IT systems, including those operated by contractors and cloud service providers, is particularly challenging when dealing with a staggering number of sophisticated cyberattacks.

Such sophisticated attacks illustrate the need for the Department to ensure a healthy cybersecurity posture, including completing the transition to zero trust architecture (ZTA). However, our audits and evaluations continue to find IT security deficiencies in the Department's IT systems and security practices. Based on our work, we believe the Department will struggle to finalize the transition to ZTA until it resolves these IT security shortcomings.

Priority areas

- Continuing the transition to zero trust
- Improving IT security shortcomings and strengthening cybersecurity

Continuing the transition to zero trust

The President's May 2021 executive order[i] established many new cybersecurity requirements and outlined an extensive path forward with the intent of improving the security of the federal government's systems. Included in this order was a goal of adopting ZTA. Zero trust principles call for additional protection checkpoints each time a user wants to access data, instead of giving full trust to insiders. Thus, even system insiders will encounter more scrutiny.[1]

The Office of Management and Budget has set a deadline of fiscal year (FY) 2024 for federal agencies to adopt ZTA, with many milestones along the way. Although the Department has made progress in implementing some ZTA requirements, such as launching a vulnerability disclosure program (which has since identified more than 300 vulnerabilities in departmental

[1] For more background information on zero trust, see our FY 2023 *Top Management Challenges* report, OIG-23-001.

systems), fully implementing ZTA remains a challenge.

For example, in our March 2023 capstone report on the Department's Active Directories, we observed that the Department had yet to implement new zero trust password requirements that were due in January 2023.[ii] Active Directories are a critical part of implementing these requirements because they serve as a centralized way to authenticate users and systems on a network. Yet none of the Department's bureaus had updated their Active Directories to enforce the new requirements at the time of our audit, and many Department systems are still noncompliant. Continuing to enforce ineffective, outdated password requirements places mission-critical services at a higher risk.

The Department is also working toward fully implementing the following key ZTA requirements, all of which have deadlines that are approaching (or already overdue):

- Enforcing user authentication through multiple factors such as passwords and physical tokens (commonly referred to as multifactor authentication or MFA) (due November 2021)
- Ensuring data is encrypted, both when being stored and in use (due November 2021)
- Implementing MFA on certain publicly accessible systems to protect against phishing attacks, in which attackers trick individuals into disclosing sensitive personal information (due January 2023)
- Implementing comprehensive device-logging and information-sharing capabilities (due August 2023)
- Deploying and maturing software that can monitor user devices to detect and respond to potential attacks (due September 2024)

The Department's MFA implementation is particularly important because of the positive effect this single control can have on IT security. During one press briefing, a deputy national security advisor reported that MFA could prevent 80 to 90 percent of cyberattacks. However, the Department still has over 100 systems that have not implemented this crucial control. On March 22, 2023, we initiated an audit of the Department's implementation of MFA on its high value assets (HVAs). This audit will identify opportunities for the selected bureaus to implement more effective MFA.

The Department needs to prioritize the completion of overdue ZTA deadlines like MFA while continuing to make progress on future ones. Traditionally, bureaus have implemented most federal IT security requirements individually, with limited support from the Department. However, the immense scope of ZTA will require extensive coordination and resources to meet the goal of full adoption by the end of September 2024.

Improving IT security shortcomings and strengthening cybersecurity

To implement a comprehensive strategy like zero trust, a strong cybersecurity foundation needs to be in place. The Department and its bureaus rely on complex systems, networks, and software to complete their missions, making proper IT security management and oversight of these assets essential. The Department must ensure it has processes and resources in place to maintain a strong, mature

cybersecurity posture. Unfortunately, we continue to identify IT security shortcomings that have hindered the Department's efforts to strengthen its cybersecurity posture.

For example, during our recent audit of the Department's identification and remediation of vulnerabilities on HVAs,[iii] we noted the Department did not always prioritize and fix exploitable critical weaknesses, leaving systems vulnerable to attackers. HVAs are the Department's most critical systems, and without them the Department's mission cannot be achieved. Although HVAs should be a priority for IT security management, we found that known exploitable vulnerabilities existed on HVAs for prolonged periods—270 days, on average—potentially allowing attackers to make these critical systems inoperable.

In fact, through our own testing we were able to successfully exploit these vulnerabilities on HVAs across several bureaus. While the bureaus attributed delays in remediating vulnerabilities to technological issues and a lack of resources, we determined that a lack of prioritization was at the center of most of the delays. To properly prioritize the remediation of HVA vulnerabilities, management will have to redirect the Department's already limited technological and staffing resources. Our report made four recommendations related to prioritizing the remediation of HVA vulnerabilities, information sharing among HVA system owners, and standardizing the scanning of systems for vulnerabilities.

In another example, our evaluation of the Office of the Secretary's Cybersecurity Incident Response Program found the program lacked proper security foundations, including tools, policies, and procedures necessary to detect and respond to a cybersecurity incident.[iv] We simulated malicious activities during our evaluation, including exfiltrating over a million fictitious sensitive records, but our actions went largely undetected because security tools, such as those that ensure data loss prevention and endpoint protection, had been poorly configured.

Even after being alerted to these issues, the Office of the Secretary's security operations center mishandled and delayed forensic activities due to a lack of procedures. While officials repeatedly attributed the identified security weaknesses to an overall lack of resources, they had not prioritized fixing the issues over the prior 2 years. Our report made 14 recommendations to the Department; as of September 2023, 12 recommendations remain open. The open recommendations deal with several important corrective actions, including reviewing firewall configurations, creating forensic procedures, and obtaining the capability to automatically aggregate security events and data. Until the Office of the Secretary implements our recommendations, it will encounter significant challenges in detecting and responding to cybersecurity incidents.

Additionally, in our 2022 evaluation of the Department's National Security Systems, we found all systems managed by the Department's National Security Solutions and Services team had not been consistently authorized to operate for considerable periods of time between 2016 and 2021.[v] This included lapses of as long as 11 months, during which systems continued to be used despite not being authorized to operate. Once again, these lapses occurred because the team lacked documented processes and procedures, and IT security staff was attempting to fill multiple roles in two separate offices.

Further, as of September 2023, all recommendations from this report remain open. Without significant investment by Department leadership, these security shortcomings will undermine the protection of National Security Systems.

Finally, the Department has made some progress in maturing its information security program based on the Department of Homeland Security's Federal Information Security Modernization Act metrics. However, our annual audit continues to find that the program is not yet mature enough to be rated "Effective." In FY 2023, we found that the Department's contingency planning metric had improved. Other metrics, such as risk management and incident response, regressed due to the issues we identified in the HVA vulnerability audit and the incident response evaluation described above.

In addition, the Department has not yet implemented our recommendation from a 2022 audit to centrally store security assessment results to better facilitate management oversight.[vi] Until the Department implements the recommendations from our audits, it will face challenges in improving its IT security program and successfully making the transition to ZTA.

Progress made and challenges remaining since FY 2023 *Top Management Challenges*

The Department and its bureaus made progress in addressing some of the challenges we identified in our FY 2023 *Top Management Challenges* report. For example, the newly released *Enterprise Cybersecurity Policy* updated and modernized Department-wide cybersecurity requirements by adopting the latest version of NIST's Security and Privacy Controls standard.

The new policy also requires bureaus to monitor core controls on IT systems to ensure their continued effectiveness. The Department also released six cybersecurity standards and two cybersecurity handbooks in FY 2023 to guide the implementation of the updated policy.

In addition to its vulnerability disclosure program, the Department has made some progress toward implementing ZTA by deploying a compliant endpoint detection and response tool. Bureaus have also continued to increase the number of systems which support MFA and encryption.

Due to the immense scope of ZTA, the Department's ZTA working group has been coordinating resources to meet the goal of full ZTA adoption. However, the Department has stated that it may not be possible to migrate all systems to ZTA by the Office of Management and Budget deadline of September 2024.

Ultimately, the Department must continue to focus on maturing its IT security programs and making concerted efforts to improve its IT security shortcomings. Until these improvements are made, consistently implementing ZTA across the Department and its bureaus will remain a struggle.

Challenge 2: Awarding and overseeing grants to expand broadband access to all Americans

Increasing access to broadband is an ongoing national challenge. As the agency responsible for broadband policymaking and administering a range of broadband and digital equity grant programs, the Department is at the forefront of this endeavor and has listed expanding affordable, high-quality broadband to every American as an objective in its 2022–2026 *Strategic Plan*.

The National Telecommunications and Information Administration (NTIA) is administering almost $49.8 billion to promote broadband access for every American through the Consolidated Appropriations Act (CAA), 2021, and the Infrastructure Investment and Jobs Act (IIJA).[vii] NTIA is responsible for overseeing six programs, all of which have different programmatic requirements but that aim to expand broadband infrastructure and promote broadband adoption and use. These programs include the Broadband Equity, Access, and Deployment (BEAD) program; Middle Mile Broadband Infrastructure Grant (MMG) program; Digital Equity Act (DE) programs; Tribal Broadband Connectivity Program (TBCP); Connecting Minority Communities (CMC) Pilot Program; and Broadband Infrastructure Program (BIP).

Program	Amount Appropriated	Grants Awarded	Amount Awarded
BEAD	$42,450,000,000	56	$255,800,458
TBCP	$3,000,000,000	191	$1,787,480,230
DE	$2,750,000,000	56	$53,607,932
MMG	$1,000,000,000	35	$930,021,354
CMC	$285,000,000	93	$262,852,127
BIP	$300,000,000	14	$282,785,260

As of July 28, 2023

Priority areas

- Ensuring funding is properly allocated and awarded to close the digital divide
- Overseeing broadband programs with challenging regulatory and NTIA requirements
- Optimizing workforce to manage increases in grant administration activities
- Implementing measures to prevent, detect, and report potential fraud and hold grantees and subgrantees accountable for performance

Ensuring funding is properly allocated and awarded to close the digital divide

The BEAD program, the largest of the new broadband programs, provides $42.45 billion for projects that will close the digital access gap for unserved and underserved locations and community anchor institutions (such as hospitals or universities). To allocate funding for BEAD, IIJA requires NTIA to use the Federal Communications Commission's (FCC's) National Broadband Map.

The FCC map provides information from Internet service providers about the services available to locations across the country, along with new maps of mobile coverage. However, Congress, state officials, and industry stakeholders have expressed concerns about NTIA's ability to correctly allocate funds to states and territories because the FCC map does not include all unserved and underserved locations. Using the FCC map could conflict with BEAD program requirements, which prioritize broadband funding for unserved and underserved locations.

In addition, although avenues exist for communities and individuals to dispute errors in the map's location and availability data, not everyone is able to file a challenge. For example, some states may be restricted from challenging the map due to contractual agreements for data used for state broadband mapping. In addition, some states and municipalities may lack the resources and expertise to file challenges. This further reduces assurance that the data is accurate.

NTIA's challenge will be to ensure eligible entities that received allocated BEAD program funding will award the funds equitably to their subgrantees so that broadband coverage will not be duplicated despite the incomplete and inaccurate FCC map.

Overseeing broadband programs with challenging regulatory and NTIA requirements

NTIA must ensure its broadband programs meet IIJA and CAA, 2021, requirements within the established timeframes. This means NTIA must successfully administer six large grant programs with complex and often very different regulatory and administrative requirements. Supply chain issues, permitting processes, connection and infrastructure considerations, and even technological advancements can all create delays or complications for NTIA and its grantees throughout the grant process.

Meeting regulatory requirements for purchasing and permitting

Supply chain issues

The Build America, Buy America Act expansion to broadband products exacerbates existing supply chain challenges in the marketplace[viii] because America does not produce key broadband components and equipment. While NTIA is proposing limited waivers to the requirement to purchase broadband essentials in America, additional action may be needed to address resource shortages and minimize supply chain challenges.

Permitting requirements and procedures

The BEAD program emphasizes building infrastructure for unserved and underserved communities, which may require permits from federal, state, tribal, and local

governments. This requirement can include a permit for (1) easement of access to government or privately owned land, bridges, overpasses, and railroads, and buried or aerial deployment; and (2) environmental and historic preservation considerations, which requires broadband projects to have a completed National Environmental Policy Act analysis and meet applicable state, local, and/or tribal government environmental and historic preservation permitting requirements.

NTIA has provided guidelines to inform applicants and eligible entities on permitting requirements and procedures to navigate the permit process. However, NTIA should also establish an oversight process to streamline the regulatory burden and simplify the deployment of broadband networks to meet IIJA requirements.

Developing requirements to ensure that funding for broadband projects is not duplicated and networks are not overbuilt

In July 2023, we alerted NTIA management to concerns related to the TBCP.[ix] We had learned during an audit that NTIA allowed tribes to self-certify in their grant proposals that they were not currently served by a broadband provider and did not have an enforceable commitment from a provider to build out broadband service on their lands. NTIA relied on these self-certifications instead of verifying that tribes' proposed coverage areas did not already have coverage and were not included in broadband awards from other federal programs.

As NTIA continues to oversee states' distribution of broadband funding and begins considering applications for the second round of TBCP funding, it must develop a reliable method for identifying awards that overlap with funding from other federal programs. It must also ensure that grant dollars are spent to further the goal of connecting every American instead of overbuilding where connections already exist.

Ensuring NTIA requirements are cost effective and sustainable

Choosing the right type of connection to close the digital divide

Broadband connections may consist of cable, fiber-optic, digital subscriber line, wireless, or satellite. IIJA is technology neutral and does not stipulate that one technology meets user needs over others, so NTIA must ensure it is approving the most cost effective, sustainable broadband deployment plans from states and territories.

Considerations for these plans vary widely, not just due to the nature of individual projects but because of the requirements of the different programs. For example, for the BEAD program, NTIA prioritizes fiber-optic connectivity for last-mile broadband projects (the "last mile" is the final leg of a broadband network, connecting the provider to a home or business). NTIA does not include satellite or unlicensed spectrum as a reliable broadband service for the unserved.[x] But the cost to run fiber-optic to homes and businesses in some unserved areas can be extremely expensive due to terrain, distance to sites, materials, and labor.

Although NTIA does allow states and territories some leeway regarding areas where deploying fiber-optic would be expensive, the cost must be extremely high.[xi] By contrast, for TBCP, NTIA allows a choice of technology that best meets tribal

needs, including fiber-optic, wireless, fixed wireless, and satellite.[xii]

Considering technological changes

Technology is constantly evolving, which can lead to concerns about whether deployed resources will still be current at the end of a broadband project and beyond. For example, a 100-megabit-per-second broadband speed requirement for uploads and downloads may meet every requirement for applications commonly used today. However, technologies that are in their infant stages now will be able to consume 50 times more data. NTIA must ensure the technology proposed in the grants it approves can sustain future technological development.

Optimizing workforce to manage increases in grant administration activities

The Department continues to face challenges with optimizing its workforce and internal resources as part of its 2022–2026 *Strategic Plan*. The new grant programs are placing additional demands on the Department's grants administration workforce, which historically has been stretched very thin. This may result in poor quality grants. In addition, shortages of experienced staff with the right skills and abilities can contribute to delays in deploying these new programs.

Since 2011, we have reported that the Department continues to face challenges regarding its acquisition and grants workforce. For example, our last two *Top Management Challenges* reports noted challenges such as the Department's inability to fill vacant positions promptly and attract and retain experienced professionals to work in locations outside the Washington, DC, metropolitan area. The Department needs to ensure NTIA can provide sufficient oversight of broadband grants even with limited time and staff.

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

FY 2023's top management challenge related to broadband continues to be relevant in FY 2024.[xiii] As NTIA has begun implementing the broadband infrastructure funding programs, certain concerns we raised in our FY 2023 report have become even more relevant.

NTIA has an ongoing responsibility to establish measures focused on preventing, detecting, and reporting potential fraud, waste, and abuse. For example, as previously mentioned, NTIA relied on tribes self-certifying that proposed coverage areas were unserved. Although NTIA relied on the tribes to have the best knowledge of the status of broadband on their own lands, NTIA must also put appropriate measures in place to protect federal dollars from fraud before disbursing grant funds. Effective measures may include

- Requiring robust certifications and representations from grantees and subgrantees. Without such certifications, it can be difficult to pursue certain remedies and ultimately hold grantees and subgrantees accountable. Carefully crafted certifications are effective tools for educating grantees on grant terms and conditions, for deterring fraud, and for seeking remedies.

- Implementing additional procedures to confirm the information in these certifications before making awards.

- Collecting data from grantees and subgrantees and leveraging data analytics. NTIA should implement an effective method to organize, format, and maintain all information generated while implementing grant programs along with the information it receives from funding applicants and grantees. This could ensure that such information is readily accessible and available to Department personnel, other federal partners awarding funding for broadband connectivity, and us. NTIA should also devote resources to periodically assessing the data for identified risk factors that are indicators of potential fraud.

- Mandating recurring antifraud training for grantees, subgrantees, and employees. Such training should include information about our office and about fraud, waste, abuse, and whistleblower retaliation. It should ideally occur before grantees receive project funding or begin work on projects. Keeping a record of training attendees is also important to ensure that compliance is achieved.

- Ensuring notices of funding opportunities and award terms and conditions include provisions for direct access by the Department and our office to grantee and subgrantee information.

- Requiring grantees and subgrantees to disclose any credible or suspected instances of fraud, waste, abuse, and whistleblower retaliation to both the Department and our office.

To address these issues, we have conducted an extensive outreach and liaison operation with NTIA personnel and applicants as well as broadband funding grantees. As part of these efforts, we have provided numerous fraud awareness briefings, addressing much of the information above in greater detail, to NTIA personnel and funding grantees. For the BEAD program, we have provided antifraud briefings to applicants and grantees from nearly all U.S. states and territories.

We plan to continue collaborating with NTIA and funding grantees and to provide outreach throughout FY 2024.

Progress made and challenges remaining since FY 2023 *Top Management Challenges*

NTIA has made progress on addressing the staffing challenge identified in our FY 2023 *Top Management Challenges* report by using funding from IIJA and CAA to hire 142 full-time-equivalent employees. In addition to educating NTIA personnel and applicants as well as broadband funding grantees, NTIA has

- hosted eight public webinars and four listening sessions in 2023

- held dozens of online meetings with state broadband offices to provide technical assistance and cohort collaboration to support state and territory planning for BEAD

- posted various technical assistance resources on its BroadbandUSA website (broadband.ntia.doc.gov), supporting applicant and grantee efforts to engage with NTIA programs as well as other, broader technical assistance resources to support community efforts supporting broadband expansion, adoption, and use

- posted a draft waiver from the Build America, Buy America Act for limited domestic manufacturing for BEAD grant programs
- proposed a 1-year exemption to certain domestic manufacturing requirements for the MMG program
- proposed a temporary general applicability public interest waiver from the Build America, Buy America Act for IIJA federal assistance awards in the Pacific Island territories.

Challenge 3: Promoting growth in domestic semiconductor manufacturing and research

Over the past several decades, the United States has lost ground as a leader in semiconductor manufacturing and research. In 1990, the United States had 36 percent of the world's chip production capacity. By 2020, this amount had fallen to only 10 percent, and none of the most advanced chip manufacturing is located in the United States.[xiv]

In 2022, Congress passed the historic Creating Helpful Incentives to Produce Semiconductors and Science Act[xv] (CHIPS and Science Act) to promote long-term growth in domestic semiconductor manufacturing and research in support of national and economic security. The CHIPS Act of 2022 (division A of the CHIPS and Science Act) authorizes direct funding (including grants, cooperative agreements, or other transactions) to support research and development, innovation, and manufacturing related to semiconductors.[2] This includes investments in facilities, workforce development, and collaboration between government agencies and private entities.

The CHIPS Act provides the Department $50 billion. Of this amount, $39 billion is available to provide incentives for investment in facilities and equipment in the United States. The remaining $11 billion is for establishing a robust domestic research and development ecosystem and overseeing a suite of programs intended to strengthen and revitalize the U.S. position in semiconductor research, development, and manufacturing. In addition, the CHIPS Act authorizes the Secretary of Commerce to issue up to $75 billion in direct loans and loan guarantees, of which $6 billion can be used to support administrative costs. The Department is implementing these requirements through the National Institute of Standards and Technology (NIST).

Priority areas

- Hiring and retaining qualified staff in a competitive labor market
- Implementing adequate internal controls and oversight

[2] The CHIPS Act of 2022 amended Title XCIX of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021; we refer to these provisions collectively as the CHIPS Act.

Hiring and retaining qualified staff in a competitive labor market

As the Department implements the CHIPS Act, both the CHIPS Program Office and CHIPS Research and Development Office must ensure they have enough staff with the necessary skills to ensure proper oversight and use of funds. To rigorously evaluate and analyze funding proposals, highly technical expertise is needed, including individuals with experience managing large federal programs, experts from the semiconductor industry, and executives with financial sector experience.

NIST will face a significant challenge in hiring and retaining qualified staff in a highly competitive labor market. According to one study,[xvi] the semiconductor industry's U.S. workforce will grow from approximately 345,000 jobs today to approximately 460,000 jobs by 2030. Even with that growth, the United States faces a shortfall of 67,000 technicians, computer scientists, and engineers in the semiconductor industry by 2030, and a gap of 1.4 million such workers throughout the broader U.S. economy.

At the same time, NIST needs to address its own internal challenges in recruitment and retention. In 2023, the U.S. Government Accountability Office[xvii] found that NIST needs to improve workforce planning to address issues such as

- competition for a highly specialized workforce
- pay that is not competitive with private sector employers
- specialized workforce knowledge that is difficult to replace promptly
- gender-related imbalances in career advancement and an unwelcome environment for women

Shortages of experienced staff with the right skills and abilities can contribute to delays in awarding funds and less oversight after funds are awarded. In response to this challenge, we initiated an audit in fiscal year (FY) 2023 to determine whether NIST has enough staff with the necessary skills to ensure proper oversight and use of CHIPS Act funds.

Implementing adequate internal controls and oversight

The CHIPS Program Office can award and administer over $39 billion in direct funding of semiconductor manufacturing incentives. The office can also administer up to $75 billion in direct loans and loan guarantees. Similarly, the CHIPS Research and Development Office will administer and award up to $11 billion in research. As new offices with substantial funding responsibilities, the CHIPS Program Office and CHIPS Research and Development Office must implement adequate internal controls and oversight of all funding agreements.

However, as described in other challenges, managing grant programs effectively is a challenge for many bureaus in the Department, including NIST. Key areas of concern include ensuring proper funding awards, overseeing the use of awarded funds, and ensuring these investments achieve intended results.

Preventing the misuse of funding for purposes that are not aligned with the CHIPS Act's goals will also pose a challenge. To protect American economic, technology, and security interests, the CHIPS Act establishes safeguards such as

- prohibiting the use of funds to construct, modify, or improve facilities outside the United States
- restricting funds from being invested in most semiconductor manufacturing in foreign countries of concern for 10 years after the funds have been awarded
- limiting fund recipients from engaging in joint research or technology licensing efforts with a foreign entity that relates to national security concerns

Moreover, the CHIPS Act outlines additional requirements related to workforce development. For example, applicants must secure commitments from educational partners to provide training and develop strategies for creating equitable workforce pathways for economically disadvantaged individuals. Applicants for such incentives under the first CHIPS notice of funding opportunity that request over $150 million in direct funding must also provide a plan for access to childcare for the children of facility and construction workers.

With all these requirements, the direct funding and loan agreements will need extensive monitoring and reporting to ensure that project recipients comply with statutes, achieve intended outcomes, and use funds efficiently. Deficiencies in these areas can lead to misspent funds, improper payments, and an ineffective program. In addition, the complexity of the transactions may make it more difficult to detect and prevent errors, fraud, waste, and abuse.

The CHIPS Act represents a major investment in the United States' semiconductor industry and workforce. Ensuring that its funds are used properly will be an ongoing challenge for the Department. To address this challenge, we plan to provide comprehensive periodic updates on the status of CHIPS Act programs. As a high-profile initiative in its early stages, the CHIPS Act will benefit from the valuable insights these reviews will offer into the program's progress and potential issues.

In addition, our Office of Investigations is working with NIST to build an outreach and liaison operation to educate NIST personnel, applicants for and recipients of funding, and other CHIPS Act stakeholders on fraud awareness and other related topics.

Challenge 4: Enhancing weather, water, and climate services

The National Oceanic and Atmospheric Administration's (NOAA's) ability to provide weather, water, and climate services is dependent on its ability to collect high-quality environmental data from satellites, ships, aircraft, and ground systems. Its specialized programs must be well-managed, keeping existing systems operational and developing new systems on schedule. To produce actionable information, NOAA also needs a skilled workforce of scientists and forecasters, reliable infrastructure, and high-performing, accurate forecast models.

The NOAA components that manage its satellite systems, ships and aircraft, and weather services are again at the core of NOAA's top management challenges for fiscal year (FY) 2024. The National Environmental, Satellite, Data, and Information Service (NESDIS) is responsible for NOAA's satellites. The Office of Marine and Aviation Operations is responsible for NOAA's fleet of ships and aircraft. Weather and climate forecasts are provided by the National Weather Service (NWS), which also collects data via ground-based systems.

Priority areas

- Maintaining a robust satellite architecture
- Ensuring successful ship replacement efforts and communicating impacts of a potential gap in high-altitude aircraft observations
- Increasing NWS' effectiveness at protecting life and property in a changing climate

Maintaining a robust satellite architecture

NOAA maintains three major satellite system architectures: polar orbiting, geostationary, and space weather. For each of these systems, NOAA's challenge is to maintain continuity of operations to ensure satellite data is available for weather models and storm tracking.

In FY 2024, NESDIS continues deploying its established satellite systems, the Joint Polar Satellite System (JPSS) and the Geostationary Operational Environmental Satellite (GOES)-R Series. The launches for the next satellites in these systems are planned for FY 2027 and FY 2024, respectively. As these systems complete their missions, NESDIS is starting to plan their replacements and develop new strategies for collecting data while

maintaining continuity of critical satellite observations. This requires NOAA to mitigate risks that could delay satellite launches or threaten operations.

Executing established programs

Managing schedule and technical challenges for completing the JPSS program

After successfully launching JPSS-2 in November 2022, the JPSS program is developing and building JPSS-3 and JPSS-4, with plans to finish both by 2026. A key performance challenge for NESDIS will be to address schedule and technical challenges to complete these satellites and ensure they are fully functional.

One of the biggest challenges for the JPSS program is the development and integration of a new instrument, Libera. This instrument will record how much energy leaves Earth's atmosphere every day, maintaining a longstanding record of climate data currently provided by legacy instruments. Originally planned for integration on JPSS-3, Libera will now be integrated onto JPSS-4 after delays in the instrument's development. To make Libera operational as soon as possible, the program decided to move JPSS-4's planned launch date up to 2027, ahead of JPSS-3's planned launch. The program now plans to finish integrating and testing JPSS-3 in 2024 but will not launch it until 2032.

Postponing JPSS-3's launch will require putting the satellite in long-term storage for 6 years on the ground. However, the program's storage plan is not complete, with important activities related to preserving the health of key components and testing yet to be detailed.

With the launch for JPSS-4 moved up, the program must also contend with the erratic behavior of the Advanced Technology Microwave Sounder (ATMS), a key instrument on JPSS satellites. The issue led the program to swap JPSS-3's faulty ATMS with JPSS-4's functional instrument, but the program must still resolve the ATMS performance problem before JPSS-4 is launched. Any delays in resolving the problem would threaten JPSS-4's now-accelerated schedule.

Launching final GOES-R series satellite and completing on-orbit testing

NOAA plans to launch GOES-U, the final satellite in the GOES-R series, in April 2024. In late FY 2023, the GOES-R program was completing GOES-U's environmental testing, which demonstrated that the satellite could meet its launch and operational requirements.

The program must now verify that the satellite can meet its requirements and pass a mission milestone in October 2023, in which a review board will assess the satellite's readiness before it is shipped to the launch site. After launch, it must undergo a series of tests. NESDIS must also decide whether to place the satellite in on-orbit storage or use it to replace one of its two operational satellites, GOES-East and GOES-West (so named because they capture storm data over the east and west coasts of the Americas).

Planning future satellite capabilities

Meeting observational requirements while evolving space acquisition philosophy and approach

NOAA is planning its next generation of polar orbiting satellites. The Near-Earth Orbit Network initiative will replace traditionally large polar satellites, such as JPSS, with smaller satellites that have fewer instruments, or only one instrument. The QuickSounder mission, expected to launch

in December 2025, will serve as a bridge between JPSS and this next generation of polar satellites.

QuickSounder represents a new approach for NOAA in more ways than satellite size. Instead of a traditional satellite program, in which NOAA contracts with a company to build a satellite that NOAA will operate, contractors will build and operate QuickSounder and provide the data to NOAA. QuickSounder aims to demonstrate that NOAA can obtain operational observations on a compressed schedule with a small, commercially operated satellite. If this mission is successful, NOAA expects to use what it has learned in fulfilling future satellite observation needs. However, NOAA must ensure that its requirements for global satellite coverage are met as it works in new ways with its internal and external partners.

Designing the GeoXO satellite system to provide the best overall mission value

The GeoXO program is a follow-on mission to the GOES-R series, planned to replace the GOES-East and GOES-West satellites. GeoXO's current plans call for satellites in the east and west positions above the western hemisphere, plus two additional satellites, launched 5 years apart, in a central location between the east and west satellites. The two central satellites will add certain capabilities to the system, including providing real-time information about the distribution of atmospheric moisture, winds, and temperature.

As discussed in our recent audit report,[xviii] with the central satellites the program expects to significantly exceed NESDIS' requirements for the satellite system's functionality. However, the central satellites' capabilities are secondary to the primary imaging mission, which the east and west satellites will fulfill. In addition, a second central satellite may not be needed to fulfill the requirements of the mission. The program needs to assess its assumptions about the mission's availability (the probability that a satellite system will fulfill its mission over time) and whether the additional performance capabilities are worth additional costs.

Focusing space weather programs on preventing data gaps

NOAA's space weather programs are racing to provide sustainable solutions to aging satellites. For example, the Deep Space Climate Observatory, launched in February 2015, is already past its expected operational lifetime. The Space Weather Follow On (SWFO) program is a bridge mission between the current systems and the Space Weather Next program, which intends to sustain, improve, extend, and mitigate potential gaps in space weather operations and data.

NOAA has entered an agreement with NASA for the SWFO satellite to "rideshare" on the launch of a NASA research mission. Because SWFO is a secondary payload for the NASA mission, NOAA must work with NASA to determine whether the two agencies can agree on needed flexibility in the research mission's launch schedule. An inflexible schedule could either delay the SWFO mission, increasing the risk of a gap in space weather measurements, or halt it altogether if the NASA mission launches without the SWFO satellite. In a recent report, we recommended further coordination between the two agencies and an update to mitigation plans for a potential gap in space weather observations.[xix]

Migrating data and services to the cloud

As part of the next-generation satellite architecture, NESDIS is migrating data storage, processing, and products to the

cloud, under the Office of Common Services. The office must address staffing shortages to meet key challenges in developing agile, scalable ground services, which involve migrating data and some capabilities to the cloud. Its challenges include achieving targeted metrics for migrating archived data, transforming data into cloud and artificial intelligence (AI)-ready formats, and developing an AI-enabled science testing environment. According to NOAA, the evolution from mission-siloed systems to enterprise services requires a business culture shift toward increased communication and collaboration across offices. New roles, responsibilities, and processes are being navigated and developed as the technology evolves.

Planning for potential loss of opportunities to purchase weather data from vendors

NOAA's Commercial Data Program began in 2016 to fund commercial pilot programs and data purchases, with the goal of improving weather forecasts and reducing risk to weather data observations. A NOAA study found that in 2021, commercially purchased data was approximately one-quarter to one-half the cost of data generated from government satellites.

Under the data program, NOAA is funding radio occultation (RO)[3] purchases, which are used to improve weather model forecasts. According to NOAA, these purchases contribute approximately 50 percent of all the RO data NOAA uses daily.

Three vendors originally offered RO data purchases, but one has stopped. Program officials have stated they are concerned that eventually only one RO vendor will remain in the marketplace, creating a monopoly and driving up prices. NOAA needs to have a plan in place to ensure the continuity and sufficiency of RO data even if purchasing the data from a vendor is no longer viable.

Mitigating risks to satellite operations

Safeguarding operations and communications from frequency interference

In our FY 2023 *Top Management Challenges* report, we noted that in FY 2022, NOAA requested funding for additional staff with spectrum expertise to address frequency interference issues. NOAA did not receive this funding in FY 2022 and asked for it again in FY 2023. Although NOAA was funded and did hire staff with spectrum expertise in FY 2023, spectrum risk remains as emerging technologies with wireless transmissions increase, such as the proliferation of 5G cellular networks. NOAA needs to be proactive in managing this risk to ensure the success of its missions.

NOAA and the National Telecommunications and Information Administration (NTIA) have identified a risk of future interference to a key frequency remotely sensed by polar weather satellites. An adjacent 5G cellular band, which is yet to be operational, is owned by commercial entities, and the Federal Communications Commission (FCC) has yet to accept lower international limits to mitigate interference. In June 2023, NTIA submitted a notice of proposed rulemaking to the FCC to explain its position on commercial use of, and risks

[3] RO uses satellites to detect changes in radio signals from a global navigation satellite system such as the Global Positioning System. These changes are created as the signals pass through the Earth's atmosphere and vary with differing atmospheric conditions, such as temperature and humidity. This allows their values to be measured, creating RO data.

associated with, this frequency band. However, the FCC has yet to make a ruling.

Additionally, the FCC authorized operation of a terrestrial radio network near the GPS frequency bands. In September 2022, a congressional study raised potential interference concerns about commercial entities pursuing the use of adjacent frequencies. NTIA reported that after this study was released, commercial interest in these frequencies ceased.

Implementing basic space situational awareness services

NOAA's Office of Space Commerce (OSC) will fulfill the Department's role, designated in Space Policy Directive-3, of providing space situational awareness and space traffic management services to commercial space operators.[xx] OSC is currently developing the cloud-based Traffic Coordination System for Space (TraCSS), which will contain an open-architecture space situational awareness data repository, a user interface, and a testing environment. OSC plans for TraCSS to provide limited space situational awareness capability to commercial and non-Defense Department government satellite operators in FY 2024, and full operational capability in FY 2025. Delivering capabilities in these timeframes is contingent on OSC addressing several challenges:

- OSC plans to pursue data standards for TraCSS. Agreement between the Department, satellite owner and operators, and service providers on standards and sensitive data are concerns.
- OSC issued contracts to collect and analyze space situational awareness data. An aggressive procurement schedule is planned in the next year.
- The Department of Defense tracks and publishes a catalog of over 40,000 space objects, but in FY 2024 this mission is transitioning to the Department of Commerce, under OSC. The two departments are still defining the details of this transition, including the availability, format, and cadence of data provided from the Defense Department.

Ensuring successful ship replacement efforts and communicating impacts of a potential gap in high-altitude aircraft observations

NOAA's ship and aircraft fleets are vital national assets for environmental observation and data collection. They inform critical products and services NOAA provides to government agencies, communities, and businesses around the country.

NOAA's Office of Marine and Aviation Operations (OMAO) operates and maintains a fleet of ships, aircraft, uncrewed systems, and small boats. These platforms have a broad array of scientific observation and data collection capabilities that play a critical role in the characterization of oceanographic, atmospheric, and hydrographic conditions, as well as assessments of fisheries and marine life, from coastal regions to the deepest reaches of the world's oceans. They also observe, collect, process, and transmit data used to predict tropical cyclone paths, landfall locations, wind intensities, storm surges, and post-storm events, thus safeguarding life and property and aiding in storm recovery.

As NOAA's fleets age, they must be sustained and recapitalized (that is, ships or

aircraft with modern equipment and capabilities must be purchased). NOAA must identify and communicate risks associated with recapitalization while developing effective long-range risk mitigation plans.

Half of NOAA's ships must be replaced within 5 years, but NOAA lacks an updated fleet plan

NOAA's most recent fleet plan, issued in 2016, identified eight ships that would reach the end of their useful service life by 2028. One of these ships has already been retired; the remaining seven have exceeded their design life as well as a service life extension. (All seven are at least 32 years old, with three being 56 years old.) If the ships are not replaced by 2028, NOAA's marine-based observation and data collection missions will suffer.

OMAO has already begun updating NOAA's fleet. Two oceanographic research ships are under construction, and a detailed design and construction contract for two hydrographic survey ships was awarded on June 23, 2023. NOAA has received appropriations nearing $600 million for these four ships. OMAO is also developing requirements for marine life and fishery survey ships.

But these efforts are underway without an updated fleet plan to replace the outdated 2016 plan. A fleet plan informs key stakeholders of the current state of the fleet, provides replacement and maintenance plans, articulates a high-level schedule for ship acquisitions and retirements, and details long-term appropriation requirements (including the amount and year funds are needed for each new ship).

According to officials, NOAA has prepared an updated draft fleet plan, which must be approved by the Department, Office of Management and Budget, and Congress. NOAA is still reviewing the plan internally but expects to submit the report to Congress in FY 2024.

By not finalizing and issuing a new fleet plan sooner, NOAA has delayed communication to its stakeholders about each ship class's technical scope, full estimated cost, and required funding over time. This creates risks in these areas to NOAA's ship recapitalization efforts. In addition, an investment in the fleet requires a significant investment in human capital for design management and shipbuilding quality assurance oversight; the lack of an updated plan impedes OMAO's ability to hire, train, and retain this workforce. NOAA is also missing an opportunity to communicate to Congress about the funding it needs to execute its plan.

Our past audits and our FY 2023 *Top Management Challenges* report have also documented the need for NOAA to update its fleet plan, as well as improve planning and governance of OMAO fleet recapitalizations and ensure that future acquisitions address user requirements.[xxi] We plan to initiate an audit on ship acquisitions in FY 2024.

"Hurricane hunter" aircraft are nearing the end of their service life

OMAO operates several highly specialized aircraft that are also rapidly approaching the end of their useful life. Its Gulfstream IV plane is the only observational system in the world equipped to collect high-altitude wind data that enables accurate 5- and 7-day hurricane forecasts. OMAO also uses the Gulfstream IV for high-altitude

collection of data on atmospheric rivers[4] such as the ones that delivered record precipitation to western states in the winter of 2022–2023. Due to the aircraft's age and reliability, OMAO plans to remove it from service in March 2025.

OMAO has initiated a program, with $164 million in appropriations, to acquire and develop the Gulfstream IV's replacement. After experiencing delays, however, the new aircraft's projected January 2025 delivery date is at risk; therefore, NOAA may not have a Gulfstream IV replacement in time to gather data for the 2025 hurricane season.

NOAA must calculate and communicate the impact of this potential data gap to stakeholders. However, it has not yet made any viable plans or established any risk mitigations to address the effects a gap would have on forecast models and public safety.

Increasing NWS' effectiveness at protecting life and property in a changing climate

In its 2023–2033 strategic plan, NWS specified goals to empower its people, improve infrastructure, and transform the agency. These goals aim to help NWS meet current and future mission needs for providing weather, water, and climate services for the protection of life and property.

As part of our FY 2023 *Top Management Challenges* report, we noted the legislative goal to improve forecasting of tornadoes and hurricanes and reduce impacts on life and property.[xxii] Since 2019, supplemental disaster relief funding and the Infrastructure Investment and Jobs Act[xxiii] have invested at least $707 million toward forecasting significant weather and climate events. Supplemental funding is still in the early phase of obligation, but NWS faces long-term challenges in staffing and infrastructure, two elements that are key to improving its performance.

Hiring and retaining a skilled workforce quickly enough to reduce vacancy rates

As we identified in our FY 2023 *Top Management Challenges* report, NWS staffing issues remain a persistent challenge. NWS' FY 2023 funding was increased by $11.75 million over its FY 2022 funding to help it meet staffing requirements. But as of the third quarter of FY 2023, NWS' workforce vacancy rates were the same or increasing among its physical science and meteorology staff.

In addition, hiring at NWS took almost twice as long as the U.S. Office of Personnel Management's 80-day benchmark. Slower hiring rates can cause heavier employee workloads, burnout, and departures, which further exacerbate the vacancy rate.

Transitioning to reliable, resilient infrastructure

After our FY 2023 *Top Management Challenges* report highlighted NOAA's tornado warning dissemination delays, NWS determined the cause of the delays was related to older software code that did not adequately perform during a network interruption. Legacy web servers are also unstable, according to NWS officials. The

[4] See https://www.noaa.gov/stories/what-are-atmospheric-rivers for an explanation of atmospheric rivers.

agency's goal is to modernize related IT infrastructure by June 2024.

NWS is also in the conceptual phase for its follow-on to the Next Generation Weather Radar system within the Department's scalable acquisition framework, standing up the program office to establish requirements and costs for replacing the legacy system without interrupting coverage. We describe NOAA's broader IT modernization efforts in challenge 5.

Improving accuracy to better adapt to society's changing needs and vulnerabilities

In the past decade, NWS has focused on social science awareness, better risk communication, and workforce transformation. However, these efforts may need to be reassessed, given the increasing number and costs of weather and climate disasters. To this end, we have initiated an evaluation of NOAA's tornado warning and forecast performance.[xxiv]

In addition, Congress established a goal to improve hurricane forecasts and warnings to reduce loss of life and economic damage.[xxv] Hurricane Ian, which struck Florida in 2022, is an example of the importance of achieving this goal. Ian had a catastrophic impact on Florida, causing an estimated $113 billion in damage—making it the third costliest hurricane on record—and 66 deaths. However, according to NOAA, its average official 2-day forecast track error for Ian was comparable in accuracy to recent years.[xxvi] Hurricane Ian's catastrophic effects showed that historic forecast performance benchmarks may not be sufficient measures for the future.

Another challenge for NWS is modernizing its climate-related model products. According to recent studies,[xxvii] NWS' flood frequency estimation products may not accurately represent climate trends, which may put communities at risk if their infrastructure is designed with incorrect flood risk profiles.

Progress made since FY 2023 *Top Management Challenges*

Our FY 2023 *Top Management Challenges* report discussed aspects of most of these same challenges. Below we summarize NOAA's progress in these areas.

Ensuring continuity of environmental satellite data

NOAA's polar and geostationary satellite programs had several major accomplishments in FY 2023. As previously mentioned, the JPSS program launched its JPSS-2 satellite on November 10, 2022. JPSS-2 completed post-launch testing and is operating as NOAA-21. And the GOES-R series program completed the bulk of GOES-U satellite-level testing as it readies for launch, planned for April 2024.

In addition, the GeoXO program received approval for the project's second and third milestones. The project moved from the formulation phase into the execution phase on December 14, 2022.

Finally, NOAA met two goals in its ongoing efforts to reduce risks to civil and commercial satellite operations. As mentioned earlier, NOAA obtained funding to increase staffing for developing a strategy to mitigate spectrum-related risks facing NOAA programs. In addition, OSC defined a proposed system architecture with roles and functions for major TraCSS components.

Recapitalizing ships and aircraft

In FY 2023, NOAA's ship and aircraft recapitalization efforts continued. In August 2022, OMAO completed and distributed an updated aircraft plan, which articulated updated requirements for all aviation operations and the future architecture of its aircraft fleet. And in June 2023, NOAA awarded a $305 million contract to design and build two hydrographic survey vessels.

Balancing weather service improvements and longer-term climate resilience

NWS made progress in several areas related to improving weather and climate services. Following a successful pilot project in the Pacific region, Weather Service Chat (a primary communication tool among forecasters and stakeholders) will finish moving to a more modern, commercial off-the-shelf platform in 2023. Additionally, on April 11, 2023, the Milestone Decision Authority approved milestone 0 for the follow-on radar program and directed NWS to work with the Department of Commerce Office of Acquisition Management to achieve milestone 1 by the first quarter of FY 2025. Finally, the Hurricane Analysis and Forecast System went into operation on June 27, 2023, and will run alongside existing models for the 2023 season before replacing them as NOAA's primary model. The system is expected to increase forecast accuracy and reduce storm impacts to lives and property.

Challenge 5: Leveraging trustworthy artificial intelligence and modernizing IT systems

Artificial intelligence (AI) is transformative technology with a wide range of applications that have the potential to improve the operations of the Department and its bureaus. To ensure mission success, AI must be ethically designed and managed to ensure public trust and confidence, with protections for privacy, civil rights, and civil liberties. As the Department's use of AI increases, it must institutionalize strong accountability and risk management frameworks to ensure safe and effective systems. AI may provide many benefits, but because AI systems can obscure direct analysis, risks can be poorly understood. By applying appropriate frameworks, the Department will better understand and monitor its AI systems to enhance services and avoid harm.

In addition, the Department is accelerating its efforts to replace or upgrade many legacy IT systems and platforms with cloud-based IT. But speeding up IT modernization can create issues with identifying requirements, estimating costs, scheduling projects, and implementing management controls. Further, while cloud-based systems can update and simplify enabling technology, the Department cannot ignore the need to plan thoroughly and reengineer its operations to achieve the greatest benefits from its new technology.

Priority areas

- Leveraging trustworthy AI to ensure safe and effective enhancements of operations and services
- Modernizing IT systems

Leveraging trustworthy AI to ensure safe and effective enhancements of operations and services

Executive order 13960, *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government,* states, "Agencies must . . . design, develop, acquire, and use AI in a manner that fosters public trust and confidence." To this end, the order established a set of principles for use of AI in government.[xxviii]

Under these principles, agencies' use of AI is expected to be (among other things) accurate, reliable, safe, secure, understandable, responsible, transparent, and accountable. More recently, the White House Office of Science and Technology Policy promoted similar principles in its *Blueprint for an AI Bill of Rights*.[xxix]

Before bureaus transition AI into key operations and services, the Department must ensure it has adequate governance and controls, in the form of policies, procedures, and practices, to ensure AI is safe and effective. To develop these controls, the Department should leverage accountability and risk management frameworks.[xxx]

As of May 2023, the Department has reported 52 use cases of AI across 8 bureaus. AI can bring many benefits to the Department. For example, natural language processing is used to interpret and help classify survey input and improve searches of the Department's public data. And machine learning algorithms are used to identify dangerous rip currents from shoreline web camera footage, map urban heat islands, and improve navigation and magnetic field forecasts.

This important and revolutionary technological progress must not come at the price of civil rights or privacy, or by limiting access to opportunities, resources, or services. The Department has a duty to protect citizens from unsafe or ineffective systems, a duty that includes designing ethical, equitable, and robust AI systems that deliver mission value, remain transparent and accountable to the public, and operate within the confines of American values and laws.

Department leadership will need to ensure that AI systems perform as expected, create reproducible results, can be independently verified, and meet all mission requirements. Other challenges include identifying and managing the existence of shadow AI (systems that operate outside of normal boundaries, such as approvals, privacy, and security, typically without management's direct knowledge), locating and addressing sources of AI bias, and ensuring appropriate levels of human supervision over AI systems.

Modernizing IT systems

To accelerate its IT modernization efforts, the Department is relying on cloud-based IT platforms. The Department's 2022–2026 *Strategic Plan* notes that using new cloud-based tools and platform features will "decrease time spent maintaining legacy systems . . . increase the efficiency and accuracy of core processes . . . automate repetitive tasks, reduce duplication . . . and standardize the tools employees use to perform their jobs." [xxxi]

While cloud-based systems can update and simplify enabling technology, merely transitioning to this new IT is no substitute for reengineering processes for better efficiency. By planning how to optimize its operations before acquiring new IT—even efficient cloud systems—the Department can achieve the greatest possible efficiency benefits for its core processes. IT modernization efforts should consider desired process efficiencies in their analyses of cloud infrastructure options (full cloud, on premises, and hybrid).

The inherent challenges of moving to cloud platforms include migrating data from legacy to new systems and ensuring the ability to retain data when cloud service contracts are terminated. The Department must consider how future system architectures enable the efficient sharing of data, improve data access and usage, and allow for the opportunity to identify and discover authoritative climate science, demographic, and geospatial data that will respond to national challenges.

Modernizing two core cloud-based financial and grants management systems is a continuing challenge for the Department in

fiscal year (FY) 2024. Other key system modernizations at several bureaus also require management attention to ensure their success.

Overseeing Business Applications Solution program performance

Effective oversight and management of the Department's Business Applications Solution (BAS) program is necessary to ensure accountability for cost, schedule, and performance targets. Currently, the program does not maintain a cost estimate or schedule in accordance with Department policy. These program management controls are necessary to identify drivers for potential cost increases, schedule delays, or system performance gaps.

The Department will transition the National Oceanic and Atmospheric Administration's (NOAA's) financial operations to the cloud-based BAS application suite on October 25, 2023, after a 1-year delay. In concert, program staff must provide support to NOAA's acquisitions, financial, and property workforces as they adapt their processes to the new system.

In prior work, we noted that the Department struggled to define target business processes.[xxxii] Implementing our recommendations will be important to ensuring an effective implementation of BAS for NOAA as well as for the Census Bureau and the National Institutes of Standards and Technology, both of which will transition their financial operations to BAS over the next 2 fiscal years.

The Department must plan and execute the work necessary to implement BAS financial applications for NIST by October 1, 2024. Improving Department-level oversight, implementing program controls, and incorporating lessons learned from the NOAA transition while addressing NIST-specific needs will be keys to success.

Implementing an enterprise grants management system that meets bureaus' needs

As noted in past *Top Management Challenges* reports, the Department intends to implement the Grants Enterprise Management Solution (GEMS), a single system to replace separate systems used by its bureaus. The GEMS implementation continues to depend on the Department's successful implementation of the BAS financial management application. However, more immediate needs, as well as unique requirements, have led some bureaus to use alternative grants management software. This presents challenges with systems and records integration, data migration, security and privacy requirements, and additional costs.

NIST has opted to use an alternative grants management system to support the immediate needs of the program that manages grants and financial assistance from the Creating Helpful Incentives to Produce Semiconductors and Science Act of 2022 (CHIPS Act). NIST's CHIPS Act grants have higher security requirements than what the GEMS program's chosen grants system can provide, which would complicate these grants' eventual transition to GEMS.

As we have reported, the U.S. Economic Development Administration (EDA) and the National Telecommunications and Information Administration (NTIA) have also adopted alternative software to support their needs,[xxxiii] which complicates the Department's implementation plans for GEMS. EDA is procuring a suite of IT services—the majority of which support

grants management—that are projected to cost approximately $33 million through 2025 and $2 million per year for operations and maintenance thereafter. Much of that cost is in addition to the estimated $75 million lifecycle cost of GEMS, of which the Department has thus far spent $14.4 million.

Ensuring success of key IT system modernizations across the Department

Other system modernization efforts across the Department require effective oversight, sound program management, and well-designed and implemented controls to ensure success.

National Weather Service systems

NOAA is modernizing and simplifying its public web page at weather.gov, increasing computing capacity of its weather prediction supercomputers, and moving its forecaster workstation system[5] to a cloud-based solution that will enable robust tools when deployed during a high impact event or other emergency.

National Environmental Satellite, Data, and Information Service's common cloud framework

As one of the Department's most critical data warehouses for environmental data, NOAA's National Environmental Satellite, Data, and Information Service seeks to modernize the storage and distribution of its data through cloud-based systems. While doing so, NOAA will face challenges such as updating business processes, establishing modernization goals aligned with new processes, selecting appropriate management methodologies, managing huge amounts of data within a cloud-hybrid architecture, and ensuring adequate security controls.

Census Bureau Business Ecosystem

As described in challenge 10, the Census Bureau is modernizing key enterprise capabilities for data collection, storage, processing, and dissemination for all surveys and data products, including the 2030 decennial census.

Patent product line

The U.S. Patent and Trademark Office is replacing critical systems used for managing its patent services. In a recent audit, we found that its cost estimating and scheduling processes were not comprehensive, and its Agile management practices needed improvement.[xxxiv]

Progress made since FY 2023 *Top Management Challenges*

The Department has made some progress addressing issues we identified in our FY 2023 *Top Management Challenges* report.

Avoiding further delays to BAS implementation

In response to a July 2022 audit report, the BAS program provided an action plan to address our recommendations identifying paths to improving its business process reengineering, requirements management, and risk management. However, it has yet to fully implement all actions, and all six recommendations remain open.

In October 2022, the BAS program implemented the property management application and part of its acquisition management application for the entire Department. After a 1-year delay, the

[5] Advanced Weather Interactive Processing System; see https://www.weather.gov/phi/TourAWIPS (accessed August 2023).

program is making final preparations to launch all three of its financial management applications at NOAA in October 2023 (beginning of FY 2024).

Managing risks to the implementation of an enterprise grants management system

After delaying its initial implementation by a year, GEMS continues to work toward implementation by March 2024 at NOAA and at the bureaus serviced by the NOAA Grants Management Division. These bureaus include the Minority Business Development Administration, the International Trade Administration, and NTIA.

As NIST, EDA, and NTIA have all opted to use alternative grants management systems, GEMS must now manage additional risks related to migrating legacy grant data, system integration, security and privacy requirements, and costs.

Challenge 6: Effectively enforcing export controls and supporting U.S. supply chain resilience

Effective export controls prevent the unauthorized use of U.S. technologies for purposes contrary to American interests. Attempts by countries of national security concern, such as China and Russia, to obtain U.S. goods and technologies for the purpose of improving their military capabilities represent a strategic national security threat, and the tactics used to illicitly acquire U.S.-origin items have become more sophisticated.

Recent world events, such as the COVID-19 pandemic and the war in Ukraine, have illustrated the dangers of concentrated supply chains in foreign countries and inadequate consideration of geopolitical risk in making sourcing decisions for U.S. companies. As a result of these recent events, U.S. supply chains were disrupted, with the U.S. economy experiencing short- and long-term supply chain shortages in a vast array of markets, from electronics to lumber. ITA analysis informs U.S. government decisions in response to supply chain crises and establishes frameworks for how the U.S. government can assess supply chain risk within emerging technology sectors.

Priority areas

- Ensuring effective enforcement of export controls to counter China's Military-Civilian Fusion (MCF) strategy
- Ensuring effective enforcement of export controls on Russia and Belarus
- Promoting U.S. supply chain resiliency through timely and impactful analysis
- Combating unfair trade practices by effectively resolving trade barriers and enforcing U.S. trade agreements

Ensuring effective enforcement of export controls to counter China's MCF strategy

U.S. trade with China involves national security risks due to China's MCF strategy. The strategy seeks to acquire U.S. technology through both licit and illicit means to help modernize China's military capabilities. We highlighted combating China's MCF strategy as a priority area in FY 2023,[xxxv] and it remains a top challenge in FY 2024.

Under the direction of the Chinese Communist Party, the MCF strategy is designed to develop the most

technologically advanced military in the world by 2049 by eliminating barriers between China's civilian research and commercial sectors and its military and defense industrial sectors. China's targeted technologies include quantum information sciences, robotics, semiconductors, aerospace technologies, biotechnology, and artificial intelligence. Many of these technologies have "dual use" (military and civilian) applications.

BIS' Office of Export Enforcement plays a critical role in combating the MCF strategy. It enforces export controls, investigates unauthorized exports that could result in criminal and administrative penalties, reviews export license applications, and recommends people and entities for the Entity, Denied Person, Military End-User, and Unverified lists. Those lists are important policy tools that help protect U.S. national security and foreign policy interests. In FY 2022, BIS reported that for investigations that primarily involved China, the Office of Export Enforcement secured 9 criminal convictions, 2 subjects found guilty at trial, 4 plea agreements, 13 criminal indictments or criminal investigations, 1 criminal complaint, 4 arrests, 2 temporary denial orders, 8 seizures, and 56 court orders.

As part of its efforts to address the threat posed by China's MCF strategy, BIS issued a rule in October 2022 amending the Export Administration Regulation (EAR). The rule restricts the export to China of specific types of semiconductors, semiconductor production equipment, items related to advanced computing, and supercomputers; BIS has determined that China's ability to develop or produce such items is a national security threat.

To address these challenges, BIS has stated that it will strengthen its enforcement program by including significantly higher penalties for serious violations that will help discourage companies from violating export control policies. BIS must also prioritize its workload to investigate enforcement cases and identify persons and entities that are violating published rules when sending U.S. technology to China.

Ensuring effective enforcement of export controls on Russia and Belarus

The Department continues to focus on U.S. trade relations and the enforcement of strict export controls on Russia and Belarus. Due to the ongoing conflict in the region, effective enforcement of export controls is an integral part of the U.S. government's efforts to meet a major U.S. foreign policy and national security goal: limiting Russia's and Belarus's access to items that could support Russia's military capabilities. In our FY 2023 *Top Management Challenge* report,[xxxvi] we highlighted as a priority area ensuring proper implementation of export controls related to Russia's invasion of Ukraine. This area continues to be a challenge in FY 2024.

In response to Russia's invasion of Ukraine, BIS imposed strict export controls on Russia and Belarus. These actions expand U.S. scrutiny of transactions related to almost any sensitive dual-use technology, software, or commodity those countries could use to support Russia's war effort, as well as imposing new rules, requirements, and restrictions for Russia and Russian

military end users.[6] As a matter of policy, BIS denies applications involving these items, many of which were not previously subject to controls when destined for Russia. As stated in our FY 2023 *Top Management Challenge* report, the ability to enforce those controls depends on the appropriate monitoring of license requirements and identification of the end use of exported items and end users subject to export controls.

Given the large increase in the number of items subject to export controls, BIS must enhance its monitoring to ensure compliance with export controls on Russia and Belarus. BIS has stated that it will strengthen its enforcement by supporting surges in end-use checks[7] related to the potential diversion of items originating in the United States and subject to export controls. BIS must also strengthen its administrative enforcement program to address increasingly sophisticated tactics used by U.S. adversaries and to deter their ability to illicitly acquire U.S. technologies.

Promoting U.S. supply chain resiliency through timely and impactful analysis

The *2023 Trade Policy Agenda and 2022 Annual Report*[xxxvii] identified bolstering supply chain resilience as a critical component of the Biden administration's policy. Since 2021, the International Trade Administration's (ITA's) office of Industry and Analysis (I&A), which is composed of trade specialists, business and industry specialists, and economists, has supported the implementation of a February 2021 executive order on America's supply chains.[xxxviii] I&A provides critical industry expertise to help U.S. companies compete abroad, strengthens global supply chains vital to these companies, advances U.S. exports and supports job creation, and screens foreign investments in the United States to protect national security.

ITA's FY 2024 budget requested $21 million and the equivalent of 40 full-time employees to establish a supply chain resiliency office within I&A. The new office would help strengthen ITA's ability to identify economic and national security risks to supply chains, provide analysis and recommendations to support policymaking to strengthen supply chains, help the U.S. government identify and secure investments in strategic emerging and legacy industries, and support U.S. industries' ability to commercialize opportunities and expand exports.

Although I&A management reported that they possess the right skillsets to support strengthening supply chain resiliency, I&A told us that in general the office faces challenges with recruiting, hiring, and retaining specialized staff. In addition, technology challenges, the high demand for analytical work from I&A customers[8] to address and counter supply chain imbalances, and U.S. trading partners' retaliatory actions could hinder its capacity

[6] The specific measures imposed by the new Commerce Control List-based license requirements added new Foreign Direct Product rules specific to Russia and Russian military end users, significantly restricted the use of EAR license exceptions, and expanded Russia's existing "military end use" and "military end user" control scope to all items subject to the EAR.

[7] End-use checks 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 the EAR.

[8] I&A customers include other ITA offices, other Department of Commerce bureaus, other government agencies, and the private sector.

to produce quicker analyses when responding to national security threats.

ITA must ensure that it provides quality, timely analysis to mitigate supply shortages and any subsequent negative economic impacts. With demand increasing for its analytical expertise related to critical supply chains, ITA needs to create data tools to support its analytical work in trade and competitiveness. ITA must also enhance its analytic capabilities to inform policy development to help strengthen the global competitiveness of U.S. industry and workers.

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

We have identified the Department's ability to combat trade barriers as a priority in our past two *Top Management Challenges* reports, and it continues to be a challenge in FY 2024. One of the strategic goals defined in the Department's 2022–2026 *Strategic Plan* addresses policies or actions by foreign governments that impede the exports of U.S. goods and services. The Secretary of Commerce has also stated that the Department is committed to holding U.S. trading partners accountable when they violate U.S. laws and trade agreements.

We are completing an audit of ITA's progress in resolving foreign trade barriers faced by U.S. companies.[xxxix] We plan to issue a final report in FY 2024.

Challenge 7: Ensuring public safety entities have the network services they need to respond effectively to emergencies

The Middle Class Tax Relief and Job Creation Act of 2012 established the First Responder Network Authority (FirstNet Authority) as an independent authority within the National Telecommunications and Information Administration (NTIA). FirstNet Authority's purpose is to ensure the building, deployment, and operation of a Nationwide Public Safety Broadband Network (NPSBN) dedicated to first responders.

On March 28, 2017, FirstNet Authority entered into a 25-year contract with AT&T for the construction and operation of the NPSBN. The contract obligates up to $6.5 billion to AT&T to deploy the NPSBN. It also permits AT&T to use Band 14 spectrum for the NPSBN for the life of the contract. Under the contract, Band 14 spectrum is used primarily for public safety; however, AT&T may use excess capacity in the NPSBN to provide commercial services. AT&T pays lease fees to FirstNet Authority for the use of NPSBN capacity. Per the Middle Class Tax Relief and Job Creation Act, part of the annual lease payments will support FirstNet Authority's operations, and the rest must be reinvested into the NPSBN for maintenance and improvements.[xl] Of the $18 billion FirstNet Authority will receive from AT&T over 25 years, approximately $15 billion is expected to be used for reinvestments.

Priority areas

- Ensuring appropriate oversight of the contract's task orders
- Ensuring AT&T is meeting its goals for NPSBN adoption and coverage
- Ensuring only eligible users have access to the NPSBN
- Ensuring FirstNet Authority's innovation and test lab benefits public safety entities

Ensuring appropriate oversight of the contract's task orders

The original contract included four task orders. Other task orders were later added to the contract using the reinvestment lease fees collected from AT&T for the use of Band 14 spectrum. The challenge of ensuring appropriate task order oversight continues from fiscal year (FY) 2023's *Top Management Challenges* report.

We have reported that FirstNet Authority's oversight of the first two reinvestment task orders was inadequate.[xli] Our current audit efforts continue to identify issues with FirstNet Authority's oversight of the contract's fourth task order, which makes up the largest portion of the original contract and exceeds the total amount obligated for the reinvestment task orders. We are including this as a continuing challenge until FirstNet Authority adequately addresses its contract oversight issues.

Ensuring AT&T is meeting its goals for NPSBN adoption and coverage

The challenge of ensuring proper NPSBN adoption and coverage also continues from FY 2023's *Top Management Challenges* report. Device connection targets measure the extent of the NPSBN's adoption, and the NPSBN contract requires FirstNet Authority to make payments to AT&T at predetermined milestones for meeting both its coverage and connection targets. If device connection targets are not met, AT&T must make disincentive payments to FirstNet Authority. Because the coverage and connection milestones are tied to payments to AT&T, FirstNet Authority must provide strong oversight of AT&T's performance to ensure that FirstNet Authority is paying only for services provided. However, as mentioned above, we issued an audit report in FY 2023 related to FirstNet Authority's inadequate contract oversight.[xlii]

We are now auditing both the NPSBN device connection and coverage targets. One audit will determine whether FirstNet Authority is ensuring that AT&T is meeting the device connection targets for each state and territory; the other will determine whether FirstNet Authority is ensuring that AT&T is achieving coverage targets for each state and territory. These audits will address whether FirstNet Authority provided appropriate oversight to ensure that it is paying only for services provided.

Ensuring only eligible users have access to the NPSBN

The NPSBN contract includes an objective for AT&T to ensure adoption of NPSBN products and services by eligible public safety entities. The NPSBN includes two categories of eligible users: primary and extended primary. Primary users include law enforcement, fire, emergency medical services, 911 operations, and emergency management entities; extended primary users include entities such as public works, hospitals, and utilities, which allow primary users to respond to emergencies effectively. The incentive payments for AT&T's performance are tied to the contract's adoption targets, and AT&T determines and reports the user eligibility and classification of each device connection.

Because AT&T receives payments based on the number of device connections and is also responsible for classifying users, FirstNet Authority must ensure that it is receiving the services it paid for and that only qualified, eligible users receive the services. If unqualified users are subscribed to the NPSBN, it may not have enough capacity for public safety entities to perform critical functions in a crisis. We plan to initiate an audit on this challenge in FY 2024.

Ensuring FirstNet Authority's innovation and test lab benefits public safety entities

Ensuring FirstNet Authority's lab in Boulder, Colorado, provides benefits and effective

value-added services to public safety, while not duplicating AT&T's contracted efforts and maintaining compliance with the Middle Class Tax Relief and Job Creation Act, is a new challenge for FY 2024.

FirstNet Authority opened its Boulder facility, which houses approximately 50 people (including 9 lab employees), in November 2016. The facility comprises the 1,076-square-foot lab as well as warehouse and FirstNet Authority office space. According to FirstNet Authority, the lab "tests public safety functionality and features unique to the FirstNet network, including quality of service; priority; preemption; enhanced situational awareness technologies and applications; and future public safety functions, services, and applications." [xliii]

While AT&T is contractually responsible for NPSBN sales, marketing, operation, and maintenance, FirstNet Authority's lab also demonstrates the NPSBN for public safety officials. In FY 2023, activities at the lab also included such activities as testing 5G public safety functionality, wireless priority services, and impact on the NPSBN of elevating public safety users to primary user status. The budget for FY 2023 was $3.6 million, and expenditures as of July were $2.5 million; the budget for FY 2024 is $4.6 million. We will initiate an audit in FY 2024 to determine whether FirstNet is ensuring the lab uses its funding effectively and efficiently to support the NPSBN.

Progress made since FY 2023 *Top Management Challenges*

At its May 3, 2023, board meeting, FirstNet Authority reported the NPSBN's progress thus far, stating that

- more than 25,000 public safety agencies were using the NPSBN via more than 4.7 million device connections
- the NPSBN maintained an inventory of more than 150 dedicated mobile assets, such as cells on wheels, to provide connectivity when normal network access is not available
- more than 200 unique cell phone applications had been approved for listing in the application catalog
- AT&T had deployed approximately 99 percent of Band 14 spectrum coverage

In our FY 2023 *Top Management Challenges* report, we identified ensuring a sound reinvestment process, appropriate task order oversight, and proper NPSBN adoption and coverage as challenges. Although task order oversight and NPSBN adoption and coverage remain challenges for FY 2024, the Department, NTIA, and FirstNet Authority have made some progress on these challenges.

FirstNet has submitted action plans to address our audit findings from FY 2023. Our audit reports described concerns about FirstNet Authority's contract with AT&T, including essential analyses FirstNet had not completed, its reliance on information from AT&T that appeared to influence the reinvestment process, and its inadequate assessment and verification of contractor performance.[xliv] We recognize that 7 out of 12 corresponding recommendations have been resolved. However, continued oversight is needed to ensure FirstNet Authority's reported successes are substantiated and its action plans are effectively implemented.

Challenge 8: Managing and overseeing contracts and grants while ensuring equitable procurement

The Department's funding for contracts, grants, and financial assistance awards has increased dramatically in recent years. In fiscal year (FY) 2022, the Department obligated more than $4 billion for contractual goods and services related to programs such as national environmental satellite services, management of coastal and ocean resources, procurement, acquisition, and construction management. In addition, grant and financial assistance awards more than doubled, from $3.26 billion in FY 2020 to $6.84 billion in FY 2022.

This increase in funding was due to the significant influx of appropriations to the Department and its bureaus to provide grants and financial assistance for emergency relief, economic recovery, and infrastructure programs. As of the third quarter of FY 2023, the Department has obligated more than $8.56 billion in contracts, grants, and financial assistance awards this fiscal year.

As the Department's funding has grown, so has its ongoing challenge of ensuring proper oversight and management of contracts, grants, and financial assistance awards. The Department must manage many high-dollar procurements and award programs while ensuring that it spends taxpayer dollars prudently and safeguards programs from fraud, waste, and abuse.

Priority areas

- Managing contract and grant awards, oversight, and program performance
- Managing, strengthening, and retaining a skilled acquisition workforce to support the Department's mission
- Ensuring equity in procurement

Managing contract and grant awards, oversight, and program performance

Throughout the federal government, procurements and grants have historically been prone to fraud and waste. Improving management and oversight in these areas remains a top priority for the Department. The need for strong management and oversight becomes even more apparent as the Department administers multiple high-dollar grant programs:

- As discussed in challenge 2, the Department received $49.79 billion to implement six grant programs to provide broadband access to all Americans. The Department's FY 2024 budget has requested an additional $20 million over 2023's amount to increase grant monitoring and oversight of its broadband program.
- As discussed in challenge 3, the Department's funding through the Creating Helpful Incentives to Produce Semiconductors and Science Act of 2022[xlv] (CHIPS Act) includes $39 billion in financial assistance awards to boost the semiconductor supply chain and industry.
- Also under the CHIPS Act, the Regional Technology and Innovation Hub Program was created to focus on economic development, promote innovation and competitiveness, and prepare American regions for growth and success in the worldwide economy. The statute authorized $10 billion for the program over 5 years. The Economic Development Administration (EDA) received close to $500 million through appropriations in FY 2023 to start the program and expects to designate at least 20 tech hubs across the country.
- EDA received another $200 million as part of the Distressed Area Recompete Pilot Program, which will provide persistently distressed communities across the country with grant funding to create and connect workers to good jobs.
- The National Oceanic and Atmospheric Administration (NOAA) requested over $7 billion for its operations, research, and facilities as well as procurement, acquisitions, and construction projects for FY 2024. This funding covers expenses related to prior hurricanes and wildfires as well as conservation, restoration, observation, and forecasting to support changes in coastal systems, fisheries, and the environment.
- The Department's FY 2024 budget request includes $15 million for EDA to oversee $2.94 billion in grants that are still available under the American Rescue Plan Act of 2021[xlvi] to aid in the nation's economic recovery from COVID-19. Although grantees can receive funds until September 2027, EDA has projected that it will run out of oversight funding in FY 2023.

To manage and oversee these programs and any related contracts, the Department must continue to strengthen its acquisition management, improve grants administration and oversight, and ensure compliance with laws and regulations. Thorough documentation and performance monitoring are essential to ensuring that the Department and bureaus provide effective oversight and comply with all applicable regulations, and that contractors and grant recipients are fiscally responsible with federal funds.

Another important component of effective oversight of this funding is training Department and bureau personnel, contractors, and grant recipients on fraud awareness and the importance of compliance. The Department should strive to ensure all current and new employees, as well as those receiving funding from the Department, receive adequate training on how to identify and report fraud in its programs.

Managing, strengthening, and retaining a skilled acquisition workforce to support the Department's mission

The U.S. Government Accountability Office has identified human capital management as a high-risk area since 2001 and has noted that agencies often experience skill gaps because of a shortfall in a talent-management activity such as workforce planning or training. Skill gaps in the field of acquisitions have been identified across the government.

The Department is embarking on or continuing several high-dollar acquisitions, such as NOAA's ship and aviation recapitalization and next generation satellite systems and the Department's implementation of two business management systems, the Grants Enterprise Management Solution and Business Application Systems. (See challenges 4 and 5 for more information about these acquisitions.) A skilled acquisition workforce is necessary to complete the new acquisitions that the Department is investing in.

However, the Department's ability to hire and retain enough skilled acquisition employees to complete its mission and provide competent management and support is an ongoing challenge. Our *Top Management Challenges* reports and the Department's Office of Acquisition Management's FY 2021 acquisition human capital report have cited several specific workforce challenges for the Department, including

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

To strengthen its acquisition workforce, the Department's goal has been to collaborate with its Office of Human Resource Management to maximize incentives and explore new strategies to recruit and retain enough acquisition professionals.[xlvii] We are reviewing challenges with acquisition workforce management as part of several ongoing audits.

Ensuring equity in procurement

On January 20, 2021, the President issued executive order 13985, *Advancing Racial Equity and Support for Underserved Communities Through the Federal Government,* calling on agencies to create a diverse and resilient federal marketplace. The President directed agencies to make federal contracting and procurement opportunities more readily available to all eligible vendors and to remove barriers faced by underserved individuals and communities.

The Department, which plays a vital role in driving U.S. competitiveness and has long declared that its mission is "to create the conditions for economic growth and

opportunity," will be a key part of meeting the administration's goals.[xlviii] According to the Department's Equity Action Plan, the Minority Business Development Agency (MBDA) will provide technical assistance and serve as a critical interagency resource for delivering on the administration's goal of increasing contracts and procurements to small disadvantaged businesses.

The administration's goal is to increase the share of contracts awarded to small disadvantaged businesses by 50 percent by 2025, an unprecedented target that is projected to translate to an additional $100 billion to the businesses over the next few years.[xlix] MBDA recognizes that contracting barriers continue to exist for minority business enterprises at the prime and subcontractor levels, and will advocate for equitable procurement practices within the Department and across the federal government.

In addition, several of the Department's programs will be faced with the challenge of ensuring that small businesses, underserved communities, and minorities are aware of the opportunities and benefits available through grants. Grant funding can create opportunities to

- expand affordable, reliable access to high-speed broadband service
- offer economic development grants that will provide technical assistance to grantees, particularly those in underserved communities
- deliver technical assistance with a focus on equity
- narrow racial wealth gaps and further support minority-owned business procurements by providing services and supporting innovative initiatives to foster economic resiliency [l]

Progress made and challenges remaining since FY 2023 *Top Management Challenges*

The Department's *FY 2022 Annual Performance Report and 2024 Annual Performance Plan* offered several performance indicators and milestones for improving its management and oversight of contracts and grants, including

- strengthening its suspension and debarment program (significant improvements include a revised referral form that has greatly simplified the referral process and a revision of the suspension and debarment handbook, currently under review)
- documenting acquisition management and grant management review findings and ensuring corrective actions plans are followed
- completing acquisition review board reviews
- expanding the number of contracting officers with digital services specialization certification
- meeting implementation milestones for a new contract writing system and the Grant Enterprise Management Solutions system[li]

We will continue to monitor the Department's oversight efforts on grants and contract awards through our audits and evaluations. We have several ongoing reviews related to the Department's oversight of grants and direct payments awarded through pandemic and disaster relief funding. Additionally, our Office of Investigations has multiple open investigations concerning potential fraud in CARES Act funding, disaster relief funding,

and the Department's grant and contract awards.

The Office of Acquisition Management implemented several new strategies to increase and develop its acquisition management workforce. For example, some offices or bureaus have offered remote work, are using direct hire authority to attract new employees, and have increased training and certification programs. In addition, to ensure consistency in workforce responsibilities, the Office of Acquisition Management defined acquisition management requirements for personnel hired directly by bureaus or programs. The FY 2022 human capital report will include current and projected acquisition staffing needs in each program or bureau based on funding increases. Additionally, an acquisition innovation lab continues to be developed to encourage and explore innovative and underused acquisition techniques and tools.

We also continue to work closely with the Office of Acquisition Management on the suspension and debarment program and consistently refer cases to the Department's suspending and debarring official for consideration. In FY 2023, we referred four cases involving six respondents to the suspending and debarring official for action. These referrals resulted in two notices of proposed debarment, two "show cause" letters, and two declinations.[9] Also in FY 2023, the suspending and debarring official issued one notice of debarment and one declination resulting from two cases referred in FY 2022.

Finally, performance indicators from FY 2023 show that MBDA exceeded many goals in working with small businesses and clients. Although MBDA reported that it did not meet some of its goals last year, such as working with exporting and manufacturing clients, future budget requests support increases to the number of new business centers aimed at assisting more businesses. Business centers provide minority entrepreneurs access to the resources they need to create jobs and drive innovation. The FY 2024 MBDA budget request totals $110 million and 134 positions to provide resources to continue implementing Minority Business Development Act of 2021[lii] and authorize several new activities to support minority businesses. With the confirmation of the first Under Secretary for Minority Business Development, the budget request builds on MBDA's FY 2023 progress.

[9] Three of the four referred cases are still in process and pending a final decision.

Challenge 9: Safeguarding intellectual property to promote innovation and economic prosperity

The United States has the world's single largest economy. Intellectual property (IP) is used in virtually every segment of that economy and directly accounts for more than 47 million U.S. jobs. The strength of the U.S. economy depends directly on the U.S. Patent and Trademark Office's (USPTO's) ability to incentivize and protect new ideas and innovation.

Patent and trademark owners are experiencing fraud and theft of IP by bad-faith actors intent on stealing ideas, which threatens the U.S. economy and the competitiveness of U.S. businesses. In a July 2023 hearing, Congress members also expressed concerns on these issues. IP theft from China alone is estimated to cost between $225 billion and $600 billion per year. USPTO will be at the forefront of efforts to safeguard IP from these threats and other new and persisting risks as it moves forward in its mission to drive U.S. innovation.

Priority areas

- Adapting to emerging technologies
- Maintaining the integrity of the patent application system and trademark register
- Improving patent and trademark quality and timeliness
- Improving critical mission support functions

Adapting to emerging technologies

As new technologies emerge at a rapid pace, USPTO will be challenged to adapt to the speed at which these technologies emerge while maintaining a balanced patent system. On a global scale, we are seeing a rise in advancements and adoption of new technologies, including artificial intelligence (AI), blockchain, quantum computing, and the metaverse, to name a few.[10]

As with the AI-related concerns discussed in challenge 5, these technologies will present both opportunities and risks. On one side, continued innovation in these technologies will enhance our country's competitiveness, economic prosperity, and national security. AI technology already exists in a wide scope of products and services used in daily life, from the

[10] *AI* refers to "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments." Pub. L. No. 116-283, § 5002 (2021).

automated assistant on your phone that responds to spoken commands to cars that can scan, interpret, and respond to the surrounding environment.

On the other side, continued growth in these technologies also raises questions and complex legal issues, including questions of ownership and IP protection. As new virtual reality technologies such as the metaverse grow more common, IP issues in the real world will extend into virtual spaces as well.[11] USPTO will be challenged to educate the public on its rights when creating and using objects in the metaverse, as well as to educate inventors on protecting their IP from misuse on these digital platforms. USPTO will need to develop policies and promote regulations that encourage and incentivize U.S. innovation in these emerging technologies while balancing the complex issues that can arise.

Internally, USPTO can use these new technologies to drive efficiency in its work. Using AI and machine learning tools to support patent classification and searches for prior art,[12] as well as image comparisons for both patents and trademarks, USPTO has an opportunity to enhance the quality and efficiency of patent and trademark examinations.

Efforts to implement this technology are underway. In September 2022, USPTO released a tool that uses AI search capabilities to help examiners search for prior art during the examination process. The tool grants examiners access to patent documents worldwide with full machine translations to English. The examiners then use these results, along with other information, to determine whether the invention is patentable.

Although these new technologies can help improve operations, USPTO must also ensure its tools are collecting accurate, high-quality information. For example, information in a prior art search is critical to the examination process and relies heavily on publicly available information. If the information gathered is inaccurate, it can affect the trustworthiness and reliability of the AI tool's search results. This becomes increasingly important as misinformation and disinformation campaigns are on the rise. USPTO will need to address these risks to ensure it continues to deliver reliable IP rights.

Maintaining the integrity of the patent application system and trademark register

The integrity of patent and trademark examination and trial proceedings are of paramount importance to the delivery of reliable IP rights and the economic health of the United States. To maintain the integrity of these IP processes, USPTO's top priorities include protecting against fraud and abuse, and improving transparency for stakeholders.

In recent years, USPTO has seen significant increases in fraudulent trademark filings, including numerous suspect applications originating outside the United States, from countries such as China. These suspect applications used a variety of fraudulent schemes, including filing applications using the name of a deceased U.S. attorney. USPTO has taken steps to address the

[11] The metaverse is a virtual reality space where users can interact with a computer-generated environment and other users.

[12] Prior art consists of information available to the public and relevant to the examined patent application. Examples include prior patents, journal and magazine articles, books, websites, and scientific papers.

improper conduct it discovers. These steps include addressing the findings from our 2021 report and clearing unused trademarks from the *Federal Register* using tools available under the Trademark Modernization Act.[liii]

However, USPTO's policies and procedures aimed at defeating problem applications have been in use for a relatively short time, and its challenge is to ensure that those procedures are coordinated, effective, and modified as needed. With a rise in new methods for defrauding inventors, USPTO will need to be vigilant in identifying and deterring those efforts without delaying the process of approving legitimate applications.

USPTO has also faced public scrutiny in recent years over the transparency of its operations, specifically relating to patent operations and patent litigation. Transparency ensures clarity and certainty around examination and post-examination processes for inventors and promotes the integrity of the patent system. For example, the Patent Trial and Appeal Board lacked clarity in the decision-making factors it considered when denying requests for patent trials, and for how it handled multiple petitions filed to challenge the same patent. USPTO recently sought public input on the determination criteria for denying trial proceedings and a range of other patent trial issues.

In the patent examination realm, USPTO has faced transparency concerns with the publication of its *Manual of Patent Examining Procedure*. The manual instructs examiners on procedures to follow when examining patent applications. USPTO publishes the manual on its website to provide applicants and the public with information on examiners' current practices. The most recent edition, published in February 2023, contained changes effective as of July 2022.[liv] When changes are delayed, applicants and their representatives lack clarity on practices and may miss information useful in preparing applications and responding to USPTO requests. Uncommunicated practice changes can lead to increased time and expense for applicants and increased work for examiners. Moving forward, as USPTO develops or clarifies policy and regulations, it will also need to ensure those changes are promptly publicized and meet both stakeholders' expectations and USPTO's mission.

Finally, because examiners and judges have a critical role in ensuring the integrity of the patent and trademark application processes, their decision-making must not be impaired. In 2022, an independent report found that USPTO's oversight of judges' work and review of their decisions lacked transparency and that management oversight affected judges' ability to operate without influence when deciding cases.[lv] USPTO has published interim guidance intended to increase transparency while it works toward enacting rules. We also have an ongoing project, which we expect to publish in fiscal year (FY) 2024, that will evaluate oversight to prevent financial conflicts by patent examiners.[lvi] As USPTO moves forward, it will need to improve transparency and openness in its operations to ensure clear and consistent decision-making and maintain public trust in the IP system.

Improving patent and trademark quality and timeliness

USPTO continues to face challenges in balancing patent examination quality and

pendency.[13] According to a USPTO quality review, 17 percent of office actions[14] in 2022 did not comply with at least one of the statutes governing patentability (e.g., novelty, obviousness, subject matter, and description). Further, a USPTO survey found that external stakeholders often thought rejections based on subject matter were not clear, consistent, and correct. Quality examination is critical for providing patent owners with reliable patent rights.

At the same time, the inventory of unexamined patent applications steadily increased in FY 2023, which will put pressure on USPTO's ability to ensure quality examination. Additional examination procedures in certain technology areas may hinder timeliness as well. For example, USPTO is exploring information sharing with the Food and Drug Administration for inventions related to pharmaceuticals and biologics. As USPTO develops these procedures, it will need to ensure they efficiently provide patent examiners with information they need to improve examination without undue delays.

USPTO faces similar challenges for trademark examination. First-action pendency, which refers to the number of months between the application filing and the examiner's first action, remains well above historical levels, reaching more than 8 months in the first quarter of 2023.[15] Pendency at this level affects applicants' ability to plan and make timely business decisions. Although the application growth rate has slowed, USPTO will face challenges as it works to bring pendency down to levels consistent with stakeholder needs while maintaining examination quality.

Improving critical mission support functions

Critical IT and administrative functions underpin USPTO's ability to carry out its mission. However, USPTO continues to face challenges with modernizing its IT systems and managing and overseeing contracts. USPTO has engaged in a large-scale transformation effort to replace its legacy IT systems; this effort includes the use of AI and machine-learning technologies, as previously discussed. However, challenges related to USPTO's execution of these modernization efforts jeopardize its long-term success.

As discussed in challenge 1, a recent OIG audit report found security weaknesses in high value IT assets, leaving those technologies vulnerable to cyberattacks.[lvii] The audit, which reviewed assets from several bureaus, found that vulnerabilities went 270 days, on average, without remediation. Inadequate IT security management hinders USPTO's efforts to strengthen its cybersecurity posture. Notably, in February 2023, USPTO—the Department's second largest operator of high value assets—asked to downgrade all of its high value IT assets. In September 2023, the Department's Chief Information Officer agreed to downgrade the majority of USPTO's high value assets. USPTO, as a central authority for collecting and processing patents and other intellectual property, will still need to be diligent about protecting these assets from cyberattacks.

In a recent audit of USPTO's legacy systems, we found that USPTO did not create key project documentation needed

[13] *Pendency* refers to the fact that the application is pending, or awaiting a decision.

[14] An office action is a document written by a patent examiner that explains why the examiner has approved or rejected a patent application's claims.

[15] For comparison, first-action pendency was 2.6 months in FY 2019.

to manage program risk and uncertainty, measure performance, and provide an accounting of all costs throughout the life of the program.[lviii] Without this documentation, USPTO is unable to address risks associated with replacing legacy systems, including increased maintenance costs and system security vulnerabilities.

USPTO also faces continued challenges in its acquisition function, particularly during the acquisition planning process. We previously reported that USPTO needed to strengthen its planning and oversight of its contract for patent data capture services to prevent unnecessary or unreasonable costs.[lix] Of the five recommendations we made, one remains open as of August 2023. In an ongoing audit, which we expect to publish in late fall 2023, we found that USPTO lacks policies or procedures that define how and when it can use the *Patent Trademark Office Acquisition Guidelines* instead of traditional federal acquisition regulations. We found that USPTO needs to strengthen its acquisition management efforts to reduce the risk of paying for services it does not need and paying more money for less value.

Progress made since FY 2023 *Top Management Challenges*

In last year's *Top Management Challenges* report, we noted challenges for USPTO in (1) improving and maintaining patent quality, (2) protecting and supporting registration processes and trademark owners, and (3) improving critical mission support functions.[lx]

To improve patent application quality and efficiency, USPTO transitioned to a new filing method for submitting application-related documents. Using DOCX, a standard word processing file format supported by applications like Microsoft Word and Google Docs, this new process allows for automated checks to prevent delays when processing applications. USPTO offered training and outreach sessions to the public as well as access to information and resources to encourage use of the new filing method. This new process is intended to improve application quality, compatibility, and increase efficiency in the patent application process.

USPTO continues to implement and process filings under the Trademark Modernization Act in its efforts to clear unused trademarks from the *Federal Register.* USPTO published a new database to house administrative and sanction orders issued and expungement and reexamination proceedings filed under the new regulations. In April 2023, USPTO reported that proceedings under the act resulted in the cancellation of 1,097 unused goods or services of 1,119 filings. Moving forward, USPTO will need to devote appropriate resources to processing these filings as it addresses its backlog of applications.

USPTO agreed with our report findings on its effort to retire legacy systems, and it is implementing corrective actions that will address recommendations we made to strengthen processes for IT investments and establish contingency plans for IT systems that are no longer eligible for manufacturer support.[lxi]

Challenge 10: Ensuring the Census Bureau provides quality data to stakeholders

The Census Bureau has to manage multiple resources to ensure the decennial (10-year) census operation is cost effective, meets data quality standards, and is executed within constitutionally and statutorily mandated timeframes. For the bureau to continue providing timely, quality data on the U.S. population and economy to its stakeholders, it must ensure that its processes and operations run efficiently. Planning for the 2030 census is currently underway, which will incorporate lessons learned from the 2020 census.

In addition to the decennial censuses, the bureau conducts recurring demographic and economic surveys. These surveys help stakeholders such as policymakers, researchers, businesses, and the public make decisions on social and economic policies and programs. The data produced by these surveys are critical in helping state and local governments obtain billions of dollars in federal funding that are allocated per population throughout the decade.

Priority areas

- Incorporating lessons learned from the 2020 group quarters count into 2030 census planning
- Ensuring survey operations help produce reliable and accurate population estimates

Incorporating lessons learned from the 2020 group quarters count into 2030 census planning

Although the vast majority of the U.S. population lives in housing units, mainly houses and apartments, 3 percent (8.2 million people in 2020) live in group living facilities. These facilities, which the bureau refers to as group quarters (GQs), include college residence halls, skilled nursing facilities, military barracks, and correctional facilities.

GQs can be difficult to enumerate because they are sometimes indistinguishable from typical housing units (as with skilled nursing facilities embedded in assisted living facilities), and their status as GQs may change between censuses (as with group homes). In the 2020 decennial census, the bureau collected information from more than 272,000 GQs, an increase of more than 60 percent from 2010. About 9 percent of these GQs either were not enumerated or had population counts of zero.

As it did for the 2010 decennial census, the bureau continued its use of residency data

provided by the GQs themselves to complete its count in 2020. However, the bureau does not have a process for verifying the accuracy of GQ-provided records. Therefore, the records may not be reliable for enumerating GQs, resulting in inaccurate counts for these types of facilities.

The bureau needs to assess any plans to check the quality of GQ administrative data soon so that it can incorporate the plans into the 2030 census's operational plan (due in December 2024).

Ensuring survey operations help produce reliable and accurate population estimates

Ensuring IT systems are ready to meet 2030 census milestones

The bureau uses multiple IT systems to carry out the decennial census as well as its recurring surveys. At an estimated cost of more than $600 million for the period of fiscal years (FYs) 2021–2024, the bureau is developing the Census Business Ecosystem, a suite of systems that together will handle all collection, processing, and dissemination of data for all surveys and data products.

The four key IT initiatives in the Business Ecosystem involve the following capabilities: (1) ingesting and collecting data, (2) managing curated data frames used to support surveys and other data products, (3) maintaining a comprehensive enterprise-wide data repository, and (4) disseminating data to the public. If implemented successfully, these initiatives will streamline processes for both surveys and non-survey-based data products. To ensure a successful implementation, the bureau needs effective governance to ensure adherence to schedules and costs.

For the 2020 decennial census, the bureau carried out an earlier IT initiative, Census Enterprise Data Collection and Processing, that was intended to support all of the bureau's survey data collection and processing functions. Although this initiative achieved some successes, it also experienced challenges. For example, the bureau reduced the scope of the initiative in 2017 to prioritize decennial census capabilities, but this came at the expense of the development of capabilities for other surveys. In addition, not all product releases were delivered according to plan, due in part to misaligned schedules that did not incorporate time needed for system testing. Finally, a high number of simultaneous acquisitions resulted in fewer acquisition staff available to provide adequate oversight. The bureau must avoid a similar outcome for the suite of systems in the Business Ecosystem.

Although efforts to fully implement the Business Ecosystem will continue beyond 2030, the system must be operational in time for a "dress rehearsal" of the decennial census environment (scheduled for April 2028, 2 years before Census Day 2030).

Ensuring American communities are represented accurately in American Community Survey estimates

The American Community Survey (ACS) is an annual survey that produces data on social, economic, housing, and demographic characteristics of the American population and communities. Each year, a random sample of approximately 3.54 million addresses throughout the United States and Puerto Rico are selected to provide household data that are used to create

annual and 5-year population estimates between decennial censuses. The ACS is the largest household survey conducted by the bureau (and second-largest household data collection operation after the decennial census). In FY 2023, it was expected to cost more than $252 million.

Challenges with the ACS include a decrease in responses, which increases the risk of bias in the estimates, and data collection issues that have necessitated corrections. As part of its efforts to address these concerns, the bureau requires effective quality control processes over data collection. In August 2023, we initiated an audit to determine whether the bureau has implemented adequate data collection procedures to ensure ACS estimates are reliable.[lxii]

Addressing hiring challenges to minimize impacts to survey data collection

For each decennial census cycle, the bureau recruits, hires, trains, and manages hundreds of thousands of temporary employees. These employees carry out field operations, such as address canvassing and nonresponse follow-up, and office operations. The bureau hired 762,000 temporary employees in 2010 and 441,000 in 2020 to complete field operations.

In addition to the decennial census, the bureau's recurring surveys (such as the ACS) are carried out by thousands of field representatives. Adequate staffing for these surveys, some of which are reimbursable (that is, done on behalf of federal agency sponsors), helps ensure that survey data is accurate and complete, validated through quality assurance processes, and used to produce estimates on time and on schedule.

Our audits of the bureau's operations highlight employee hiring and retention issues. The bureau itself has also documented concerns about hiring for the 2020 decennial census. Hiring for decennial operations will likely take precedence as 2030 approaches, which may slow down hiring efforts for the bureau's non-decennial surveys.

In our recently issued report on the quality of the data from the bureau's reimbursable surveys,[lxiii] we found that the bureau identified difficulties in meeting hiring goals for field representatives, who collect data by interviewing people or households at select addresses. We also noted that high resignation numbers contributed to lower response rates in reimbursable surveys. In July 2023, we initiated an evaluation of the bureau's recruitment, hiring, and retention of employees in mission-critical positions.[lxiv]

Progress made since previous *Top Management Challenges*

FY 2023 report

Our FY 2023 *Top Management Challenges* report included four challenges for the bureau to support 2030 census planning efforts and enhance its overall survey quality. The bureau has made the following progress addressing these challenges.

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 bureau has been working on more than 60 studies—assessments, experiments, evaluations, quality control results, and a

topic report—of the decennial's programs and operations. As of July 2022, the bureau had planned to complete and publicly release 27 of the studies by the end of August 2023. However, as of September 19, 2023, the bureau has released just 16 studies. We initiated an evaluation of the bureau's 2020 Census Experiments and Evaluations Operation to determine whether the bureau prepared adequate and timely operational assessments that included the appropriate metrics to support planning for the 2030 decennial's research and testing. We plan to issue a report with our findings in early FY 2024.

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

The bureau's Post-Enumeration Survey found in 2022 that the U.S. population was undercounted by 0.24 percent (approximately 782,000 people) in the 2020 decennial.[16] This result is not statistically different from the 2010 overcount of 0.01 percent (approximately 36,000 people). In addition, six states experienced statistically significant undercounts when taking into account their net coverage error rates, while eight others experienced statistically significant overcounts. Members of historically undercounted demographic groups also saw their undercounts increase. In June 2023, we initiated an audit of the 2020 Post-Enumeration Survey to assess the validity of the survey's results as they relate to overcounts and undercounts.[lxv]

Enhancing the accuracy and reliability of the bureau's address list

The bureau is addressing recommendations from a 2019 report by the U.S. Government Accountability Office as well as a 2022 internal report, for improvements to its Local Update of Census Addresses operation.

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

In August 2023,[lxvi] we reported that the bureau needs to improve its performance management processes and quality assurance program for reimbursable surveys. We also found the bureau did not relieve field representatives from their survey data collection duties while they were undergoing falsification investigations. Our report included 15 recommendations for addressing these issues; the bureau concurred with our recommendations and is working to implement them.

FY 2022 report

Our FY 2022 *Top Management Challenges* report included three challenges for the bureau to establish a strong framework for designing the 2030 census and improving operations over surveys and employee background investigations. Audit work related to one challenge continues.

Ensuring advertising efforts increase response rates

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

[16] This figure is not statistically different than zero when taking into account a standard error of 0.25 percent.

Challenge 11: Protecting funds awarded under the Public Wireless Supply Chain Innovation Fund grant program

The Public Wireless Supply Chain Innovation Fund[lxviii] was established in 2021 to promote and support commercial development and deployment in the 5G equipment market and to drive adoption of secure, multi-vendor, standards-based, interoperable wireless networks.[lxix] The 5G marketplace is greatly consolidated and dominated by a few vendors, which can reduce resilience and security in the supply chain, play a role in higher prices, and make it difficult for new vendors to enter the market. The Innovation Fund aims to support the United States' leading position in the telecommunications ecosystem, reduce costs for consumers and operators, enhance competition, and strengthen the nation's telecommunications supply chain.

In August 2022, the Creating Helpful Incentives to Produce Semiconductors and Science Act (CHIPS Act) appropriated $1.5 billion for grants under the Innovation Fund.[lxx] The National Telecommunications and Information Administration (NTIA), as the agency responsible for administering the Innovation Fund, began awarding the grants in fiscal year (FY) 2023. Now NTIA faces the challenge of meeting an ambitious award timeline while ensuring it has strong internal controls in place to award grants properly and prevent, detect, and report fraud.

Priority area

- Implementing strong internal controls to meet timelines and ensure funds are properly awarded

Implementing strong internal controls to meet timelines and ensure funds are properly awarded

Working through the National Institute of Standards and Technology (NIST) Grants Office, NTIA planned to award up to $140.5 million in Innovation Fund grants (with most grants expected to be between $250,000 and $50 million). Eligible applicants include for-profit and nonprofit companies, colleges, industry groups, and consortiums of these entities. NTIA posted a notice of funding opportunity, the first of several planned, for the grant program on April 12, 2023, and received 144 grant applications by the June 2, 2023, deadline. Awards began just 2 months later, in August 2023.

This expedited timeline necessitates strong internal controls to ensure awards comply with the CHIPS Act, eligibility requirements, and regulations. NTIA's challenge for FY 2024 is establishing and implementing a

comprehensive control framework to ensure funds are appropriately awarded and recipients are using the funds consistent with the Innovation Fund's objectives. At the same time, NTIA must implement appropriate measures to prevent, detect, and report potential recipient fraud. As NTIA continues the award process, it must provide clear guidance, implement clear criteria for evaluating applicants, and ensure funding is awarded only to applicants that meet the criteria.

This new challenge is further complicated by another key responsibility for NTIA: expanding broadband access across the nation. As discussed in challenge 2, NTIA is administering six grant programs, totaling almost $49.79 billion, aimed at helping ensure that every American has high-speed Internet access. Administering either the Innovation Fund or the broadband grant programs would be challenging. But the requirement to manage both efforts simultaneously, within such limited timeframes, significantly increases the burden on NTIA and heightens risks related to ensuring federal dollars are effectively distributed and overseen.

Our oversight to address this challenge will include determining the steps taken to award and disburse funds, the challenges faced during the award process, and the status of awards and disbursements. In addition, we will continue to work with NTIA, NIST, and other stakeholders to increase awareness on deterring, detecting, and reporting potential fraud impacting the Innovation Fund.

Challenge 12: Ensuring strong oversight and effective use of funding for NIST construction and maintenance

The National Institute of Standards and Technology's (NIST's) scientific research is critical to our nation. It not only affects our national security but contributes to innovative manufacturing that helps drive the U.S. economy. In fiscal year (FY) 2024, NIST faces the new challenge of effectively overseeing and managing funding for construction and maintenance of its facilities, including expansion and renovation projects, even as it continues to promote U.S. innovation and technological competitiveness.

Reports from NIST's Visiting Committee on Advanced Technology[17] have raised concerns for several years, most recently as of March 2023,[lxxi] about the critical state of NIST's facilities. Also in 2023, an extensive study by the National Academies of Sciences, Engineering, and Medicine (NASEM) gained national attention when it concluded that NIST's facilities, which date back to the 1950s, are outmoded and dilapidated.[lxxii] Further, NIST's research facilities, including its mission critical laboratories, overwhelmingly fail to meet the Department's own standards for acceptable building conditions.

The poor state of NIST's facilities hinders its work and puts the nation at risk, including the nation's reputation as a global scientific leader. It also creates safety and health concerns for NIST's workforce. The NASEM study comes at a time when a separate study, funded in part by the U.S. State Department, indicates that China now leads the world in 37 out of 44 critical and emerging technologies[lxxiii]—a potential consequence of NIST facilities' conditions.

Priority areas

- Prioritizing complex construction and maintenance projects
- Ensuring prudent financial management and oversight of funds

[17] The Visiting Committee on Advanced Technology of the National Institute of Standards and Technology is a Federal Advisory Committee Act committee. It reviews and makes recommendations on general policy for NIST's organization, budget, and programs within the framework of national policies set by the President and Congress. The committee submits an annual report to the Secretary of Commerce for submission to Congress.

Prioritizing complex construction and maintenance projects

The NASEM study concludes that NIST's inadequate facilities threaten its mission performance by causing substantive delays in key national security deliverables, scientific research, and services to U.S. industry customers. The facilities' poor state has also led to costly equipment damage, estimated in the millions of dollars.

Laboratories specifically suffer from a variety of issues, including climate control, plumbing, and unreliable power. For example, NIST was months late in delivering critical equipment to the U.S. Department of Homeland Security because it could not control the humidity in its laboratory. In another instance, power outages damaged a $6 million microscope beyond repair. Such conditions have caused productivity losses of up to 40 percent for NIST researchers, due to rework and workaround efforts.

Historically, NIST has not received consistent, significant funding to execute multiple large construction and maintenance projects. Further, the facilities' issues will take years to rectify, and current funding may not be sufficient. NIST will need to ensure it has a plan to prioritize its construction and maintenance projects—a plan that considers (among other things) national security interests, critical emerging technologies, and cost-benefit analyses.

Ensuring prudent financial management and oversight of funds

As NIST continues to play an essential role in helping the United States stay competitive in critical and emerging technologies, it must also ensure strong oversight and effective use of its funds.

NIST will face significant pressure to quickly address the poor condition of its facilities. However, it will be important for NIST to practice prudent financial management and adequately oversee its funds. For example, NIST will need to ensure that construction contracts are awarded fairly and in compliance with applicable requirements. Contracts must also be closely monitored to ensure performance requirements are met, improper payments are avoided, the federal government is protected from harm, and contractors and subcontractors are held accountable.

NIST recognizes the importance of addressing these deficiencies and has developed a 12-year coordinated recovery plan to fund major modernizations while improving its facilities' conditions and functionality. This plan, which is dependent on sustained, long-term funding from Congress, budgets $300 million to $400 million annually for the construction and major renovation projects that are critical to NIST's current research priorities. It also allocates $120 million to $150 million annually to safety, capacity, maintenance, and major repairs to prevent further physical deterioration and functional obsolescence. As NIST begins implementing the plan, our office will monitor and review its progress in addressing this challenge.

Appendix A: Related OIG publications

This list presents our publicly available fiscal year (FY) 2023 work related to the top management and performance challenges facing the Department in FY 2024. These products can be viewed at www.oig.doc.gov.

Challenge 1: Continuing the transition to zero trust to overcome IT security shortcomings and strengthen cybersecurity

- *Simulated Internal Cyber Attack Gained Control of Critical Census Bureau Systems* (OIG-23-004-I; November 22, 2022)
- Capstone report: *Effective Reviews Are Needed to Enhance the Security Posture of the Department's Active Directories* (OIG-23-013-A; March 8, 2023)
- *Fundamental Deficiencies in OS' Cybersecurity Incident Response Program Increase the Risk of Cyberattacks* (OIG-23-017-I; March 22, 2023)
- *Security Weaknesses in the Department's Mission-Critical High Value IT Assets Leave the Assets Vulnerable to Cyberattacks* (OIG-23-030-A; September 28, 2023)

Challenge 2: Awarding and overseeing grants to expand broadband access to all Americans

- *Semiannual Report on NTIA's Broadband Programs* (OIG-23-009; January 24, 2023)
- Management alert: *NTIA's Reliance on Self-Certification Increased Fraud Risk for the Tribal Broadband Connectivity Program* (OIG-23-022-M; July 10, 2023)
- *Semiannual Report on NTIA's Broadband Programs* (OIG-23-024; August 21, 2023)

Challenge 4: Enhancing weather, water, and climate services

- *Space Weather Follow-On (SWFO) Program: Rideshare Schedule Presents Challenges and Lack of Backup Option Warrants NOAA Attention* (OIG-23-015-A; March 13, 2023)
- *Satellite Integration and Test Phase Improvements Are Needed to Ensure the Success of Future Polar Weather Satellite Missions* (OIG-23-027-A; September 5, 2023)
- *The GeoXO Program: Cost and Schedule Baselines Are Established, But NOAA Should Evaluate Plans for the Central Satellite Mission and Revise Its Approach to Performance Gains to Provide the Best Overall Value* (OIG-23-028-A; September 20, 2023)

Challenge 7: Ensuring public safety entities have the network services they need to respond effectively to emergencies

- *FirstNet Authority Could Not Demonstrate Investment Decisions Were the Best Use of Reinvestment Funds or Maximized the Benefits to Public Safety* (OIG-23-005-A; November 28, 2022)
- *FirstNet Authority Failed to Provide Adequate Contract Oversight for Its Initial Two Reinvestment Task Orders* (OIG-23-012-A; March 1, 2023)

Challenge 8: Managing and overseeing contracts and grants while ensuring equitable procurement

- *NTIA Took the Necessary Steps to Implement the Requirements for Awarding Funds Under the Consolidated Appropriations Act, 2021* (OIG-23-019-I; April 24, 2023)
- *EDA Implemented and Followed the Requirements for Awarding and Disbursing CARES Act Funding Through the Revolving Loan Fund Program* (OIG-23-021-I; May 24, 2023)
- *EDA Generally Maintained Grant Award Files During the COVID-19 Pandemic* (OIG-23-029-I; September 26, 2023)

Challenge 9: Safeguarding intellectual property to promote innovation and economic prosperity

- *USPTO Needs to Improve Oversight and Implementation of Patent Classification and Routing Processes* (OIG-23-026-A; August 30, 2023)

Challenge 10: Ensuring the Census Bureau provides quality data to stakeholders

- *The Census Bureau Can Improve Processes to Promote Transparency of Cooperative Agreements* (OIG-23-011-I, February 27, 2023)
- *The Census Bureau Needs to Improve its Performance Management Processes and Quality Control Program for the Reimbursable Surveys Program* (OIG-23-025-A; August 30, 2023)

Appendix B: References

[i] 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 June 5, 2023).

[ii] Department of Commerce Office of Inspector General (DOC OIG), March 8, 2023. Capstone report: *Effective Reviews Are Needed to Enhance the Security Posture of the Department's Active Directories*, OIG-23-013-A. Washington, DC: DOC OIG.

[iii] DOC OIG, September 28, 2023. *Security Weaknesses in the Department's Mission-Critical High Value IT Assets Leave the Assets Vulnerable to Cyberattacks*, OIG-23-030-A. Washington, DC: DOC OIG.

[iv] DOC OIG, March 22, 2023. *Fundamental Deficiencies in OS' Cybersecurity Incident Response Program Increase the Risk of Cyberattacks,* OIG-23-017-I. Washington, DC: DOC OIG.

[v] DOC OIG, 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.

[vi] 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.

[vii] Pub. L. No. 116-260, 134 Stat. 1182; Pub. L. No. 117-58, 135 Stat. 429.

[viii] Murphy, John G. January 2023. U.S. Chamber of Commerce: *How Extending the Reach of "Buy America" Rules Can Backfire on U.S. Workers, Companies.* Available at https://www.uschamber.com/regulations/how-extending-the-reach- of-buy-american-rules-can-backfire-on-u-s-workers-companies (accessed August 11, 2023).

[ix] DOC OIG, July 10, 2023. Management alert: *NTIA's Reliance on Self-Certifications Increased Fraud Risk for the Tribal Broadband Connectivity Program,* OIG-23-022-M. Washington, DC: DOC OIG.

[x] Broadband Equity, Access, and Deployment (BEAD) notice of funding opportunity (NOFO), 28.

[xi] BEAD NOFO, 13.

[xii] Tribal Broadband Connectivity Program NOFO, 5.

[xiii] DOC OIG, October 13, 2022. *Top Management and Performance Challenges Facing the Department of Commerce in Fiscal Year 2023,* challenge 4: "Ensuring Prudent Financial Management and Oversight of Broadband Infrastructure Funding," OIG-23-001, 19–21. Washington, DC: DOC OIG.

[xiv] Congressional Research Service, April 25, 2023. *Frequently Asked Questions: CHIPS Act of 2022 Provisions and Implementation,* 3. Washington, DC: CRS. Available at https://crsreports.congress.gov/product/pdf/R/R47523 (accessed August 10, 2023).

[xv] Pub. L. No. 117-167, 136 Stat. 1366 (2022).

[xvi] Semiconductor Industry Association, in partnership with Oxford Economics, July 2023. *Chipping Away: Assessing and Addressing the Labor Market Gap Facing the U.S. Semiconductor Industry.* SIA and OE. Available at https://www.semiconductors.org/wp-content/uploads/2023/07/SIA_July2023_ChippingAway_website.pdf (accessed July 25, 2023).

[xvii] U.S. Government Accountability Office (GAO), February 2023. *National Institute of Standards and Technology: Improved Workforce Planning Needed to Address Recruitment and Retention Challenges,* GAO-23-105521. Washington, DC: GAO. Available at https://www.gao.gov/assets/820/817831.pdf (accessed April 19, 2023).

[xviii] DOC OIG, September 20, 2023. *The GeoXO Program: Cost and Schedule Baselines Are Established, but NOAA Should Evaluate Plans for the Central Satellite Mission and Revise Its Approach to Performance Gains to Provide the Best Overall Value,* finding I, OIG-23-028-A. Washington, DC: DOC OIG.

[xix] DOC OIG, March 13, 2023. *Space Weather Follow-On (SWFO) Program: Rideshare Schedule Presents Challenges and Lack of Backup Option Warrants NOAA Attention,* finding I, OIG-23-015-A. Washington, DC: DOC OIG.

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

[xxi] DOC OIG, November 12, 2019. *NOAA's Office of Marine and Aviation Operations Needs to Improve the Planning and Governing of Its Ship Fleet Recapitalization Efforts,* OIG-20-006-A; 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; and DOC OIG, October 13, 2022. *Top Management and Performance Challenges FY 2023,* challenge 2: "Ensuring Continuity of Environmental Data from Satellites, Ships, Aircraft and Ground-Based Systems and Improving Weather and Climate Services," OIG-23-001.

[xxii] Pub. L. No. 115-25 (2017), sections 103 and 104.

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

[xxiv] DOC OIG, August 1, 2023. Announcement Memo: *Evaluation of NOAA's NWS Tornado Forecasting and Warning Performance,* #2023-461. Available online at https://www.oig.doc.gov/Pages/Evaluation-of-NOAAs-NWS-Tornado-Forecasting-and-Warning-Performance.aspx (accessed August 17, 2023).

[xxv] Weather Research and Forecasting Innovation Act of 2017, Pub. L. No. 115-25 (2017).

[xxvi] NOAA, April 3, 2023. *National Hurricane Center Tropical Cyclone Report, Hurricane Ian,* AL092022, 14. Available online at https://www.nhc.noaa.gov/data/tcr/AL092022_Ian.pdf (accessed August 2023).

[xxvii] NOAA, January 21, 2022. *Analysis of Impact of Nonstationary Climate on NOAA Atlas 14 Estimates,* 6. Available online at

https://hdsc.nws.noaa.gov/pfds/files25/NA14_Assessment_report_202201v1.pdf (accessed August 7, 2023).
See also First Street Foundation, June 26, 2023. *The 8th National Risk Assessment, the Precipitation Problem.* Available online at https://report.firststreet.org/8th-National-Risk-Assessment-The-Precipitation-Problem.pdf (accessed August 7, 2023).

[xxviii] See https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government (accessed August 15, 2023).

[xxix] See https://www.whitehouse.gov/ostp/ai-bill-of-rights/ (accessed August 2023).

[xxx] GAO, June 30, 2021. *Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities*. Washington, DC: GAO. Available online at https://www.gao.gov/assets/gao-21-519sp.pdf (accessed July 2023); and
National Institute of Standards and Technology, January 20, 2023. *Artificial Intelligence Risk Management Framework,* AI RMF 1.0. Washington, DC: NIST. Available online at https://doi.org/10.6028/NIST.AI.100-1 (accessed July 2023).

[xxxi] DOC, n.d. *Strategic Plan 2022–2026,* 65, 75. Washington, DC: DOC. Available at https://www.commerce.gov/sites/default/files/2022-03/DOC-Strategic-Plan-2022%E2%80%932026.pdf (accessed August 16, 2023).

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

[xxxiii] DOC OIG, October 13, 2022. *Top Management and Performance Challenges FY 2023*, 17–18.

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

[xxxv] DOC OIG, October 13, 2022. *Top Management and Performance Challenges FY 2023,* 23.

[xxxvi] DOC OIG, October 13, 2022. *Top Management and Performance Challenges FY 2023,* 24.

[xxxvii] United States Trade Representative, March 2023. *2023 Trade Policy Agenda and 2022 Annual Report of the President of the United States on the Trade Agreements Program.* Washington, DC: USTR.

[xxxviii] White House, February 24, 2021. Executive Order 14017: *Executive Order on America's Supply Chains*. Washington, DC: White House.

[xxxix] DOC OIG, July 16, 2021. Announcement memorandum: *Audit of ITA's Efforts to Resolve Foreign Trade Barriers* (#2021-410). Washington, DC: DOC OIG. Available at https://www.oig.doc.gov/OIGPublications/Audit-of-ITAs-Efforts-to-Resolve-Foreign-Trade-Barriers.pdf (accessed October 5, 2023).

[xl] Pub. L. No. 112-96, §§ 6208(b), (d).

[xli] DOC OIG, March 1, 2023. *FirstNet Authority Failed to Provide Adequate Contract Oversight for Its Initial Two Reinvestment Task Orders*, OIG-23-012-A. Washington, DC: DOC OIG.

[xlii] DOC OIG, *FirstNet Authority Failed to Provide Adequate Contract Oversight,* OIG-23-012-A.

[xliii] See https://www.firstnet.gov/sites/default/files/FirstNet%20Innovation%20and%20Test%20Lab.pdf (accessed August 2, 2023).

[xliv] DOC OIG, November 28, 2022. *FirstNet Authority Could Not Demonstrate Investment Decisions Were the Best Use of Reinvestment Funds or Maximized the Benefits to Public Safety*, OIG-23-005-A. Washington DC: DOC OIG; and DOC OIG, *FirstNet Authority Failed to Provide Adequate Contract Oversight,* OIG-23-012-A.

[xlv] Pub. L. No. 117-167, Div. A & B, 136 Stat. 1366, 1372, 1405.

[*xlvi*] Pub. L. No. 117-2, 135 Stat. 4.

[xlvii] DOC Office of Acquisition Management, FY 2021. *Acquisition Human Capital Report*. Washington, DC: DOC.

[xlviii] DOC, April 14, 2022. *Equity Action Plan*, 2. Washington, DC: DOC. Available at https://www.commerce.gov/sites/default/files/2022-04/DOC-Equity-Action-Plan.pdf (accessed August 2023).

[xlix] DOC, *Equity Action Plan,* 12.

[l] DOC, *Equity Action Plan*.

[li] DOC, n.d. *2022 Annual Performance Report and 2024 Annual Performance Plan*, Washington, DC: DOC. Available at https://www.commerce.gov/sites/default/files/2023-04/DOC-FY22-24-APPR-Final.pdf (accessed August 2023).

[lii] Pub. L. No. 117-58, Div. K, 135 Stat. 429, 1445.

[liii] 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.

[liv] USPTO. February 2023. *Manual of Patent Examining Procedure,* 9th ed., rev. July 2022. Available online at https://www.uspto.gov/web/offices/pac/mpep/index.html (accessed June 13, 2023).

[lv] GAO, December 2022. *Patent Trial and Appeal Board: Increased Transparency Needed in Oversight of Judicial Decision-Making*, GAO-23-205336. Washington, DC: GAO.

[lvi] DOC OIG, February 13, 2023. Memorandum: *Evaluation of Ethics Oversight in Preventing Financial Conflicts of Interest by USPTO Patent Examiners,* 2023-049.

[lvii] DOC OIG, September 28, 2023. *Security Weaknesses in the Department's Mission-Critical High Value IT Assets Leave the Assets Vulnerable to Cyberattacks*, OIG-23-030-A. Washington, DC: DOC OIG.

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

[lix] 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. Washington, DC: DOC OIG.

[lx] DOC OIG, *Top Management and Performance Challenges FY 2023*.

[lxi] DOC OIG, July 20, 2022. *USPTO Cost Estimating, Schedule, and Agile Practices,* OIG-22-026-A.

[lxii] DOC OIG, August 23, 2023. Announcement: *Audit of U.S. Census Bureau American Community Survey*, 2023-463. Washington, DC: DOC OIG.

[lxiii] DOC OIG, August 30, 2023. *The Census Bureau Needs to Improve Its Performance Management Processes and Quality Control Program for the Reimbursable Surveys Program*, OIG-23-025-A. Washington, DC: DOC OIG.

[lxiv] DOC OIG, July 25, 2023. Announcement: *Evaluation of U.S. Census Bureau Workforce Recruitment, Hiring, and Retention,* 2023-457. Washington, DC: DOC OIG.

[lxv] DOC OIG, June 14, 2023. Announcement: *Audit of the U.S. Census Bureau's 2020 Census Post-Enumeration Survey Results,* 2023-456. Washington, DC: DOC OIG.

[lxvi] DOC OIG, August 30, 2023. *Census Bureau Reimbursable Surveys Program,* OIG-23-025-A.

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

[lxviii] William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 9202(a)(1) (2021).

[lxix] Pub. L. No. 116-283, 134 Stat. 4788-4789 (2021).

[lxx] Pub. L. No. 117-167, § 106(a)(1) and (2) (2022).

[lxxi] Visiting Committee on Advanced Technology, March 2023. *2022 Annual Report*. Gaithersburg, MD: Visiting Committee on Advanced Technology.

[lxxii] National Academies of Sciences, Engineering, and Medicine, 2023. *Technical Assessment of the Capital Facility Needs of the National Institute of Standards and Technology*. Washington, DC: The National Academies Press.

[lxxiii] Australian Strategic Policy Institute, 2023. *ASPI's Critical Technology Tracker. The Global Race for Future Power.* Washington, DC: ASPI.

To report fraud, waste, abuse, or
whistleblower reprisal
in the Department of Commerce,
visit our hotline page
or call us toll free at
(800) 424-5197.

U.S. Department of Commerce
Office of Inspector General
Washington, DC 20230