

Top Management and Performance Challenges Facing the Department of Commerce in FY 2025

October 16, 2024

Report OIG-25-001



U.S. Department of Commerce
Office of Inspector General



INFORMATION MEMORANDUM FOR SECRETARY RAIMONDO

FROM: Jill Baisinger, Acting Inspector General, (202) 794-7788

DATE: October 16, 2024

CC: Don Graves, Deputy Secretary of Commerce
Chris Slevin, Chief of Staff
James Secreto, Deputy Chief of Staff
Tonya Williams, Chief of Staff
Brian Epley, 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
Patrick Sweeney, Commander
Operating Unit Heads
Operating Unit Audit Liaisons

RE: **Statement of the Top Management and Performance Challenges Facing the Department of Commerce in Fiscal Year 2025**
Report No. OIG-25-001

The Office of Inspector General is required to report annually the most serious management and performance challenges facing the U.S. Department of Commerce and to briefly assess progress in addressing those challenges.¹ Pursuant to the same statute, the Inspector General's statement summarizing those challenges is to be included in the Department's *Annual Financial Report*.

In keeping with these requirements, I have attached to this statement the final report on the Department's top management and performance challenges for fiscal year 2025. In summary, the report identifies three overarching challenge areas as well as specific issues associated with those broad topics.

- **Challenge Area 1: Modernizing Technology and Systems**
 - Maximizing Cybersecurity and IT Security
 - Modernizing IT Systems and Operations
 - Integrating AI and Other Emerging Technologies Safely

¹ 31 U.S.C. § 3516(d).

- **Challenge Area 2: Providing Core Services and Data**
 - Ensuring Secure, Fair International Trade
 - Maintaining and Improving NOAA Operations and Services
 - Safeguarding Intellectual Property and Fostering Innovation
 - Ensuring Quality Population Data
- **Challenge Area 3: Managing Spending**
 - Strengthening Oversight in Response to Dramatic Growth
 - Strengthening Oversight of the Hollings MEP Program
 - Managing Major Broadband Grant Programs
 - Managing and Overseeing CHIPS Funding
 - Overseeing the NPSBN Program
 - Overseeing NIST Facility Improvement Project Contracts

We will continue to inform the Department's decision makers of areas for improvement identified through our audits and investigations so that timely corrective actions can be taken. We will also identify, as appropriate, progress made by the Department in these areas.

We appreciate the cooperation we have received from the Department. If you have any questions about this report or wish to discuss our conclusions, please contact me at (202) 794-7788.

Introduction and Approach

This report presents our summary of the most serious management and performance challenges facing the U.S. Department of Commerce and its bureaus in fiscal year (FY) 2025. It also includes our assessment of the progress the Department has made to meet these challenges. We base our conclusions primarily on our audits, evaluations, and investigations from recent years (see the appendix for a list of relevant public reports).

About This Report

The *Top Management Challenges* report is divided into three sections that broadly reflect the Department's major challenge areas:



Modernizing Technology and Systems

Strengthening IT security posture and modernizing IT systems and operations.



Providing Core Services and Data

Providing essential information to stakeholders on such varied subjects as trade, weather and environment, intellectual property, and population data.



Managing Spending

Funding and managing major programs while protecting funds from risk, fraud, and waste.

Why This Matters

The Department plays a central role in implementing efforts to advance the nation's economic and technological leadership. It must also provide top quality data and services to its stakeholders. Recent funding increases to assist in these efforts create challenges of their own.

If the Department does not address these significant challenges, it will struggle to successfully implement its priorities and to meet its mission of creating conditions for economic growth and opportunity for all communities.

Contents

Section 1: Modernizing Technology and Systems	1
Maximizing Cybersecurity and IT Security	1
Modernizing IT Systems and Operations	2
Integrating AI and Other Emerging Technologies Safely	5
Section 2: Providing Core Services and Data	7
Ensuring Secure, Fair International Trade	7
Maintaining and Improving NOAA Operations and Services	9
Safeguarding Intellectual Property and Fostering Innovation	11
Ensuring Quality Population Data.....	13
Section 3: Managing Spending	15
Strengthening Oversight in Response to Dramatic Growth	15
Strengthening Oversight of the Hollings MEP Program.....	18
Managing Major Broadband Grant Programs.....	19
Managing and Overseeing CHIPS Funding	21
Overseeing the NPSBN Program	22
Overseeing NIST Facility Improvement Project Contracts.....	23
Appendix: Relevant OIG Reports and Ongoing Projects	25
References	30



Section 1: Modernizing Technology and Systems

The Department and its bureaus need up-to-date technology, systems, and equipment to safeguard data and provide valuable services. This is particularly important as the Department continues to implement critical programs intended to ensure American innovation, progress, and prosperity.

The Department has faced difficulties in upgrading its IT security posture, replacing legacy systems, safely integrating new technologies into its operations, and developing future generations of satellites and other resources. The Department must also increase its focus on oversight of its major modernization projects.

Maximizing Cybersecurity and IT Security

IT systems are the foundation of almost all modern-day business processes. They provide convenience and efficiency in many different settings, from allowing a member of the public to quickly contact a federal agency to helping civil servants fulfill their mission.

Despite their convenience, these always-on, always-available systems can provide a trove of data for nefarious entities and individuals looking to exploit these systems and data. The Department, like all federal agencies, must balance the need to provide appropriate access to IT systems with the need to prevent intrusion by bad actors.

Zero Trust: The Way Forward

In May 2021, an executive order was issued to modernize federal data security.¹ The related

Office of Management and Budget (OMB) memorandum imposed a requirement on all federal agencies to adopt zero trust architecture (ZTA).²

Zero trust architecture: A comprehensive security model that, instead of implicitly trusting users, requires additional protection checkpoints each time a user wants to access data.

As we noted in our *Top Management Challenges* report in FY 2024,³ the Department is working toward fully implementing several ZTA requirements. Although the Department has continued to make progress over the past year in areas such as identity management, incident detection and response, and ZTA network architecture, it has yet to fully implement all capabilities needed to support its ZTA efforts.

Historically, bureaus have implemented most federal IT security requirements themselves, with limited support from the Department. However, the scope of ZTA will continue to require extensive coordination, prioritization, and resources at the Department level, along with heavy bureau involvement, to meet the goal of full adoption.

The FISMA Challenge: Effective Security Through Program Maturity

Under the Federal Information Security Modernization Act (FISMA), federal agencies' inspectors general use a set of metrics to assess the maturity, or effectiveness, of agency IT security programs.

Although we have seen improvement in some areas, our annual FISMA audit of the Department's information security program continues to find that the program is not yet mature enough to be rated effective.

FISMA Metrics: Supporting the ZTA Transition

FISMA's maturity metrics cover core IT security domains, including identity and access management, incident response, and risk management. Identity and access management includes the key ZTA principle of *multifactor authentication* (MFA), which ensures that only authenticated users can access systems. Incident response means the agency is able to respond when an incident is detected on a device.

In the past 5 years, the Department has not improved its identity and access management FISMA score. Shortcomings in this area, along with risk management and incident response, have also been identified in our work, which continues to reflect the hurdles the Department must overcome before it can achieve full ZTA adoption:

- In our January 2024 report on implementing MFA on the Department's *high value assets* (HVAs—its most critical systems),⁴ we observed that none of the five systems we reviewed had fully implemented all zero trust MFA requirements. In fact, we were able to test and exploit weak MFA implementation on one system.
- In our September 2023 report on identifying and remediating HVA vulnerabilities,⁵ our testing uncovered sensitive system passwords that had not been protected through encryption (a key ZTA principle). Given the significance of HVAs to the Department's operations, ZTA implementation should be prioritized.
- In our March 2023 report on the Office of the Secretary's Cybersecurity Incident Response Program,⁶ we found the office often could not detect our simulated attacks and did not respond properly when attacks were detected. Our findings lowered the Department's FY 2023 FISMA score.

In addition, 23 of our reports' IT-security-related recommendations, some dating back to 2019, are still open. The recommendations relate to key issues including password authentication, MFA, vulnerability remediation, and information sharing.

Unless the Department improves its foundational IT security program, adopting ZTA will remain a challenge.

Modernizing IT Systems and Operations

Federal agencies often face challenges in effectively managing and overseeing IT program modernizations, which have historically run behind schedule, exceeded budgets, and failed to meet objectives.⁷ The Department is no exception.

The Department and several of its bureaus have embarked on major projects intended to modernize financial and grants management systems, environmental and weather data capabilities, census data collection, and patent services.

Weaknesses in oversight can create risks in executing these programs on time, keeping them within budget, and ensuring their full functionality. Our work establishes that the Department must provide more robust oversight of major ongoing modernizations if it is to meet these challenges.

BAS and GEMS: Modernizing Systems Amid Delays, Cost Increases, and Project Management Challenges

The Department is implementing two IT programs, the Business Applications Solution (BAS) and the Grants Enterprise Management Solution (GEMS), that are intended to consolidate and modernize its aging, disconnected financial systems and functions. Both systems' implementations have been affected by delays, cost increases, and incomplete functionality.

The BAS program is critical to the Department's efforts to modernize its financial management processes and infrastructure. But since BAS' initiation in 2020, the Department has twice delayed its implementation (by a year each time). Program costs have increased from \$341 million to at least \$403.3 million.

The contract increases also account for additional production support stemming from the Department's decision to customize BAS' financial applications. Additionally, when the Department launched BAS at the National Oceanic and Atmospheric Administration (NOAA) in October 2023, it was not completely functional, creating significant challenges for the bureau.

The GEMS program seeks to consolidate and modernize the Department's legacy grant-making systems into an enterprise platform. However, because GEMS relies on BAS' financial interface, BAS' delays postponed full implementation of GEMS by at least 2 years. Currently, GEMS is operational for NOAA, the Minority Business Development Agency, the International Trade Administration, the U.S. Census Bureau, and some National Telecommunications and Information Administration (NTIA) grants. Implementations for other bureaus' grants are pending.

As a result, the other bureaus have purchased other software so they can process and manage grants while GEMS is implemented. This creates challenges with system and records integration, data migration and management, and security and privacy, all of which will bring additional—potentially significant—costs to the Department.

The Department has been challenged to implement best practices for managing both programs, even as we made recommendations for improving BAS program management:

- In 2021, we issued a management alert highlighting significant risks with the Department's BAS program management approach, which prioritized implementing BAS' IT components over reengineering mission support processes.
- In 2022 and 2024, we issued two audit reports on the program, making 12 recommendations for improving program management and execution.⁸

As of June 2024, the Department had not taken action sufficient for us to close six audit recommendations from 2022, and it was still planning actions for our six recommendations from 2024. We are also auditing the GEMS program to assess its management and implementation.

The Department's challenges in implementing BAS and GEMS show that a successful transition to new IT requires examination and reengineering of business processes. Although new systems can simplify and enhance operations, they cannot succeed without a solid foundation to support their improvements. By planning how to optimize its operations before acquiring new IT, the Department can achieve the greatest possible benefit.

NOAA Satellites: Preparing for a New Generation

NOAA is modernizing its satellite operations, with new and upgraded technologies and instrumentation for its next generation of satellite systems. The Geostationary Extended Observations (GeoXO) program is its largest procurement, with a projected lifecycle cost of \$19.6 billion.

To avoid increased risk to the schedule, spacecraft and instruments' contract awards must occur as planned. However, NOAA has stated that budget uncertainties are driving the program to replan its contract activities, and the program will need to reassess scenarios that impact performance capabilities or delay procurements.

NOAA is also using new procurement practices, acquisition approaches, and commercial engagements to reduce costs and increase efficiency. The Near Earth Orbit Network program, for example, is pursuing an affordable and adaptable portfolio of observing systems. The first of the program series, QuickSounder, uses a rapid procurement approach that is new for NOAA. With NOAA's space weather satellite, Deep Space Climate Observatory, past its operational lifetime, the Space Weather Follow On and Space Weather Next programs have announced that they plan to continue, improve, and expand space-based observational capabilities, including partnering with other satellite programs.

As NOAA pursues these innovative partnerships and approaches, it must apply sound acquisition, system engineering, and development management practices. If NOAA cannot sufficiently mature its new instrument technology and improve its management practices in time, current satellite systems may need to operate beyond their planned service life, putting critical data for weather forecast models at risk.

Ongoing System Enhancements: Strong Oversight Needed to Ensure Success

Other system modernizations across the Department require effective oversight, sound program management, and well-designed, well-implemented controls to stay on schedule and ensure long-term success.

A common cloud framework at a key environmental data warehouse. NOAA's National Environmental Satellite, Data, and Information Service (NESDIS) is implementing cloud-based solutions intended to modernize its data storage and distribution and improve the functionality of its satellite ground systems and other observing systems. Challenges include updating business processes, establishing appropriate requirements, improving project management, managing huge amounts of data within a cloud-hybrid architecture, and ensuring adequate security controls.

Our August 2024 report on NESDIS' ground system transition finds that NESDIS is not following fundamental project management practices, thus reducing project oversight and accountability.⁹ We also found cybersecurity assessment deficiencies and security weaknesses that leave the system vulnerable to cyberattack and put critical data at risk.

Improving usability of National Weather Service systems. NOAA is modernizing and simplifying its [public web page](#), increasing computing capacity of its weather prediction

supercomputers, and moving its interactive weather forecast preparation system¹⁰ to a cloud-based solution that is intended to enable robust tools when deployed during a high-impact event or other emergency.

A new business ecosystem to consolidate census operations. The Census Bureau is developing a suite of systems that together will handle all collection, processing, and dissemination of data for censuses and surveys, including the 2030 decennial census. The bureau must complete this complex modernization in time for the 2030 census’s “dress rehearsal” in April 2028. However, in an earlier enterprise-wide IT initiative called the Census Enterprise Data Collection and Processing program, the bureau did not develop reliable cost and schedule estimates, increasing the project’s risk of cost overruns, delays, and unmet performance goals.

Updating patent product line systems. The U.S. Patent and Trademark Office (USPTO) is replacing critical systems that manage its patent services. In a 2022 audit, we found that its cost estimating and scheduling processes were not comprehensive and its agile management practices needed improvement.¹¹ USPTO still has not reported to us that it has taken actions sufficient for us to close one of the report’s recommendations.

Integrating AI and Other Emerging Technologies Safely

A December 2020 executive order established an ambitious set of principles for use of artificial intelligence (AI) in government. In October 2023, a second order established a government-wide effort to guide responsible AI development and deployment.¹² Under these orders, agencies’ AI use is expected to be accurate, reliable, safe, secure, understandable, responsible, transparent, and accountable. The White House Office of

Science and Technology Policy articulated similar principles in its *Blueprint for an AI Bill of Rights*.

Effective oversight of this new technology involves ensuring ethical design and use, developing standards and guidance, and proposing regulations and requirements. In addition, USPTO, as the agency charged with protecting intellectual property for the nation’s innovators and inventors, faces specific challenges in adopting AI and other emerging technologies.

AI in Government: Ensuring Quality and Accountability

AI can bring many benefits to the Department. For example, the Department identified that natural language processing can interpret and help classify survey input and potentially improve searches of the Department’s public data, while machine learning algorithms can identify dangerous rip currents, map urban heat islands, and improve navigation and magnetic field forecasts.

But the White House’s Office of Science and Technology Policy has stated that technological progress cannot come at the price of civil rights or privacy, or by limiting access to opportunities, resources, or services. The Department must design 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.

As of May 2024, the Department has reported 52 AI use cases. As bureaus transition AI into their key operations and services, the Department must put in place policies, procedures, and practices that will provide adequate governance. To do this, the Department 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.

The National Institute of Standards and Technology (NIST) recently published four new publications that cover more aspects of AI. They include two guidance documents¹³ for generative AI,¹⁴ one draft document promoting transparency in digital content,¹⁵ and a plan to develop global AI standards.¹⁶

Generative AI: A class of AI model that emulates input data to generate derivative, synthetic content such as images, videos, audio, text, and other digital content.

These publications further cement the Department's and NIST's lead role in creating government-wide standards. However, much of this guidance is voluntary.

By using AI best practices described in the NIST publications¹⁷ and others, both the Department and the government overall will be prepared to obtain AI benefits while addressing its new and specific risks.

USPTO: Emerging Technologies and Intellectual Property

On a global scale, USPTO has seen a rise in advancements in and adoption of new technologies, including AI, blockchain, quantum computing, and the metaverse. As new technologies and related intellectual property continue to rapidly emerge, USPTO must adapt while maintaining a balanced, fair, and effective patent system.


As we discussed in a 2022 audit, USPTO has engaged in a large-scale effort to replace its legacy IT systems.¹⁸ USPTO's effective execution of these modernization efforts, including the use of AI and machine-learning technologies, is critical to its ability to adjudicate ever-increasing volumes of intellectual property data.

For example, we found that USPTO did not create key project documentation needed to manage program risk, measure performance, and provide a cost accounting through the life of legacy systems. Without this documentation, USPTO cannot address the risks associated with replacing the systems, including maintenance costs and security vulnerabilities. USPTO will also need to be diligent about protecting its systems from cyberattacks.

In addition, continued growth in emerging technologies raises complex legal issues. USPTO has acknowledged the importance of educating the public, including inventors, on their rights when creating and using these technologies. Developing policies and promoting regulations can encourage U.S. innovation in these emerging areas while balancing the complex issues that can arise.

USPTO is also exploring the use of AI and machine learning to enhance the quality and efficiency of its patent and trademark examinations. For example, it is developing new tools to support patent classification and searches for prior art and to conduct image comparisons for patents and trademarks.

If USPTO is to meet its goal of delivering reliable intellectual property rights, it must ensure its new tools are collecting accurate, high-quality information. USPTO has requested comments from the public on how AI's proliferation could affect some of its evaluations.



Section 2: Providing Core Services and Data

The Department manages a great variety of services that are essential to the nation and the world. Our trade with other countries, our inventions and creations, our weather data and environmental observations, our population and demographic data—all of these rely on the Department and its bureaus.

The complexity of the Department’s mission and operations adds to the complexity of its challenges in these areas. How the Department addresses these challenges could affect the United States’ economic success and its relationships with the rest of the world.

Ensuring Secure, Fair International Trade

At the forefront of U.S. trade enforcement and promotion are two of the Department’s bureaus, the Bureau of Industry and Security (BIS) and the International Trade Administration (ITA).

These bureaus must balance the need to protect U.S. goods and technology from foreign adversaries with the drive to resolve trade barriers and promote trade between the United States and other countries.

BIS: Improving Operations to Safeguard U.S. Technologies

Foreign adversaries and countries of national security concern often try to acquire U.S. commodities, software, and technology to strengthen their military capabilities. Moreover, BIS has expressed concern that in

the wrong hands these tools may be used to abuse human rights. According to BIS, these efforts present a strategic threat to U.S. national security. Effective export controls are critical to preventing the unauthorized use of U.S. goods and technologies for purposes that conflict with U.S. national security and foreign policy interests.

In 2022, BIS implemented new export controls and significantly expanded existing controls on Russia and China to restrict their access to U.S. goods and technologies. BIS took these actions to respond to Russia’s invasion of Ukraine and to counter China’s Military-Civilian Fusion strategy, which supports China’s goal of developing the most technologically advanced military in the world by 2049.

BIS’ actions have greatly increased the number of U.S. goods and technologies that are subject to export controls and added hundreds of foreign parties to the Entity List to restrict their abilities to obtain U.S. items,

which has led to a corresponding increase in BIS' workload. Moreover, procurement networks associated with Russia and China have adopted increasingly sophisticated tactics to evade export controls and illicitly obtain goods and technologies originating in the United States. To address these challenges, BIS has taken several actions to strengthen its enforcement, such as:

- Increasing monitoring to ensure compliance with its enhanced export controls
- Prioritizing its workload to investigate enforcement cases

BIS should also minimize the risk of unauthorized release of U.S. controlled advanced computing and semiconductor manufacturing technology and software source code to China. In a September 2024 audit, we reported that BIS' approval process for export licenses adequately reduces the risk that U.S. controlled items would be inappropriately approved for export to China and potentially used to support China's military advancement.¹⁹ However, we also found that BIS, in consultation with other federal agencies, made a policy decision to exclude certain deemed exports and reexports from regulatory licensing requirements.

Deemed export: Any release in the United States of controlled technology to a foreign person. The release is “deemed” an export to the person’s most recent country of citizenship or permanent residency.

As a result of the exclusion, U.S. companies do not need an export license to release certain advanced computing and semiconductor manufacturing technology or source code to Chinese nationals in the

United States. This could increase the risk of release of these technologies and software to China, which could help further the Military-Civilian Fusion strategy and enhance China's military capabilities.

In our audit report, we recommended that BIS take proactive steps, such as developing a mitigation plan, to minimize risks to U.S. technologies and software. BIS concurred with the recommendation, stating it was planning additional outreach to companies that are subject to the advanced computing and semiconductor manufacturing licensing requirements discussed in the report.

Foreign Trade: Ensuring Barriers Are Effectively Resolved

Foreign governments can impose trade barriers—policies, practices, or procedures that unfairly or unnecessarily restrict U.S. exports—on the United States. Addressing policies or actions by foreign governments that impede the exports of U.S. goods and services is one of the strategic goals in the Department's *FY 2022–2026 Strategic Plan*.

However, in a November 2023 audit report, we found that ITA did not effectively resolve foreign trade barriers to increase exports of U.S. goods and services or ensure American businesses and workers have equal opportunities to compete in foreign markets. Specifically, ITA did not strategically manage trade barrier cases, report complete and accurate trade barrier information in its case management system, or accurately report performance measures to U.S. companies working to resolve trade barriers.

We made eight recommendations to ITA for improving the effective resolution of trade barriers. ITA has developed an action plan to address our recommendations.

Maintaining and Improving NOAA Operations and Services

NOAA faces operational challenges as it executes its environmental data collection mission. The challenges are related to maintaining its current satellite capabilities, improving weather operations, managing ship and aircraft fleet acquisitions while minimizing and mitigating gaps in mission continuity as obsolete platforms are retired, and developing a system to provide space situational awareness and space traffic management services.

Environmental Satellite Systems: Maintaining Reliable Capabilities Until the Next Generation Is Launched

NESDIS manages NOAA's major satellite systems: the Geostationary Operational Environmental Satellite (GOES)-R series and the Joint Polar Satellite System (JPSS). With the launch of GOES-U, the last satellite in the GOES-R series, the constellation of geostationary satellites will be fully in place. NOAA will need to maintain robust constellation health until their replacements, the GeoXO satellites, are launched. (We discussed GeoXO and other new systems and programs in section 1, "Modernizing IT and Operations.")

The JPSS program is now building JPSS-3 and JPSS-4—the final satellites in the JPSS series—with plans to finish developing and testing both satellites by 2026 and subsequent storage on the ground until ready for launch. A key challenge for the JPSS program will be to retain its staff's knowledge while JPSS-3 is in long-term storage to ensure that issues do not occur once it is needed for launch and operation.

These satellite systems must perform as needed and be maintained until their

replacement systems are launched. Otherwise, NOAA may not be able to provide accurate, timely weather forecasts and warnings.

Weather Services: Increasing Effectiveness at Protecting Life and Property in a Changing Climate

Improving the accuracy and timeliness of the National Weather Service's (NWS') weather forecasts is not a new concern. It requires increasingly complex improvements to infrastructure and technology at a time when the bureau faces intensifying demands on its capabilities.

Modernizing NWS has been a priority for many years. Between 1989 and 2000, NOAA received an estimated \$4.5 billion to modernize and restructure NWS. By 2018, NOAA had implemented a multiyear supercomputer upgrade for weather, water, and climate forecast models that increased storage capacity by 60 percent and processing speed by 50 percent. In 2023, NWS launched the Hurricane Analysis and Forecast System to accelerate improvements in forecasting hurricanes.

In FY 2024, NWS again identified the need for significant infrastructure improvements to enhance its ability to do its work and communicate with the public. This follows other recent issues, including a 2022 network service interruption that led to delayed tornado warnings in Iowa and an April 2024 backup system failure that affected radar, alerts, and warning disseminations for 5 hours.

NWS has stated that it is trying to make its networks less susceptible to failure by replacing router equipment at its data centers, and it has requested an FY 2025 budget increase of \$11.4 million to improve system reliability. NWS is also transitioning critical infrastructure to the cloud so it can increase service quality during high-demand periods.

In addition, NWS has worked to improve how and what it communicates to the public in its forecasts. For 2024, the National Hurricane Center is testing a change to its threat “cone” graphic, to incorporate recommendations from social science research, that is intended to better specify risks while not increasing the graphic’s complexity.

Making these improvements is increasingly complex because demands on NWS’ capabilities and resources have mounted over the years. And, as we noted in our FY 2024 *Top Management Challenges* report and in recent interviews with NOAA leadership, workforce recruitment, retention, and burnout continue to be issues the agency has to manage.

Ships and Aircraft: Reducing Risk of Gaps in Critical Observational Capabilities

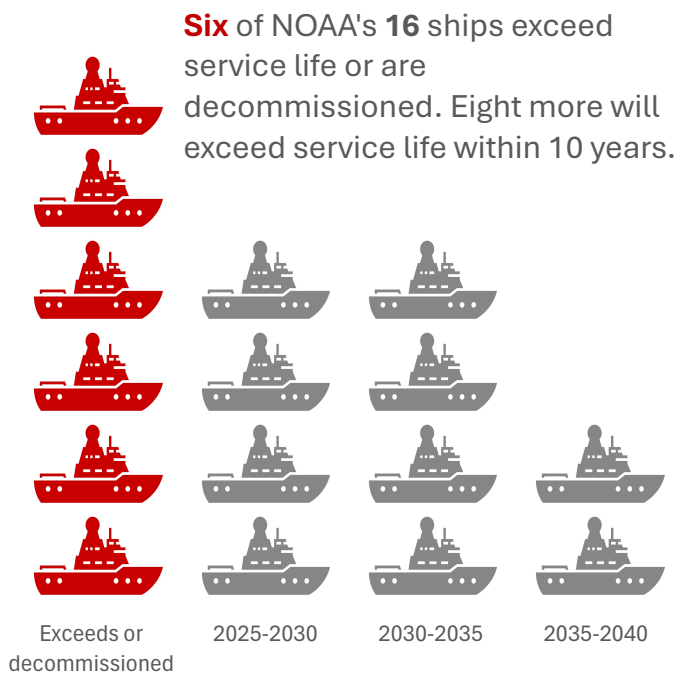
As we reported in our FY 2024 *Top Management Challenges*, NOAA’s Office of Marine and Aviation Operations is undertaking efforts to recapitalize its ship and aircraft fleets.

Recapitalization: The process of retiring old units and replacing them with new ones that are optimized for current requirements and missions.

In addition to the reduced reliability, obsolescence, and increased maintenance costs of aging assets, challenges with these recapitalizations pose a threat to NOAA’s ability to deploy observational platforms and fulfill its mission objectives.

We alerted NOAA management to concerns regarding the sufficiency of its ship construction program when compared to the requirements in NOAA’ fleet plan.²⁰ In

particular, we expressed concern that the construction program is not keeping up with the need for observational vessels and proposed that NOAA should address this issue to ensure that it can continue fulfilling its mission effectively.



In addition, NOAA operates two types of “hurricane hunter” aircraft, one that conducts low-altitude flights into storms to determine their intensity and one that collects data at a high altitude on the storm track. This data is crucial to accurate hurricane forecasting. As an example, the rapid intensification of Hurricane Otis in October 2023 was only identified when a low-altitude hurricane hunter flew into the storm.

Accuracy in forecasts enables state and local authorities to direct evacuations before a storm’s landfall. Without data from hurricane hunter aircraft to support forecasts, the risk to those in the path of severe weather will increase. The delivery schedule for the new high-altitude aircraft puts NOAA’s ability to conduct high-altitude surveillance missions during the 2025 hurricane season at risk.

These issues will require NOAA to make important decisions about acquisition planning, initiating acquisitions in time to replace aging ships and aircraft, and adequately overseeing its acquisition programs. NOAA must also proactively improve its asset management, increase its long-range recapitalization planning, and regularly update its ship and aircraft fleet plans. Only by doing so can NOAA ensure that it is able to continue providing essential services and fulfilling its strategic objectives in the years ahead.

Space Traffic Risks: Basic Services for Civil and Commercial Satellite Operators

NOAA's Office of Space Commerce (OSC) is responsible for coordinating the Department's space-related issues, programs, and initiatives. In December 2022, Congress appropriated \$70 million for OSC to develop an enterprise solution for ingesting, archiving, processing, and disseminating space situational awareness (SSA) data to space operators.²¹

Space situational awareness: The knowledge and characterization of space objects and their operational environment to maintain safe, stable, and sustainable space activities.

OSC is using an agile approach to develop the system, now called the Traffic Coordination System for Space (TraCSS).²² The TraCSS program roadmap in December 2023 indicated its initial SSA capability would be delivered to civil and commercial space operators by the fourth quarter of FY 2024. However, our July 2024 report finds that OSC is behind schedule in developing TraCSS. We also found OSC has made only limited progress in developing a new space traffic management

(STM) approach to mitigate the increasing risk of collisions in space.

Space traffic management: The planning, coordination, and on-orbit synchronization of activities to enhance the safety, stability, and sustainability of operations in the space environment.

At present, OSC is primarily focused on TraCSS' initial capability, which includes the first step toward STM services, specifically data notifications to space operators. However, we concluded that OSC lacks a plan to fulfill its long-term vision for STM-related responsibilities. We recommended that OSC develop a realistic timeline to effectively manage TraCSS, assess its progress, and communicate credible expectations to stakeholders.

Additionally, we found that OSC's lack of a long-term plan for its STM-related responsibilities may delay the development of a new approach to mitigate the increasing risk of collisions in space, which could jeopardize orbit availability and, potentially, human life. Accordingly, we recommended that OSC define and document its approach to its short- and long-term STM-related responsibilities and develop a plan for fulfilling them.

Safeguarding Intellectual Property and Fostering Innovation

Providing quality, timely patent and trademark rights is a USPTO core function. Balancing quality and pendency in patent and trademark examinations was reported in our FY 2024 *Top Management Challenges* and remains an ongoing challenge.

USPTO has also seen increased fraud and abuse surrounding patent and trademark applications, and the U.S. Government Accountability Office (GAO) has identified a lack of transparency in making patent decisions.

Patent and Trademark Review: Improving Quality and Timeliness

According to a USPTO quality review, approximately 17 percent of the office's actions in 2023 did not comply with at least one of the statutes governing patentability. Indeed, as we reported in our 2024 *Top Management Challenges*, USPTO showed similar results in a 2022 quality review. Further, a USPTO survey found that external stakeholders often thought patent rejections based on subject matter were not clear, consistent, and correct.

At the same time, the inventory of unexamined patent applications steadily increased in FY 2023. USPTO is developing additional examination procedures in certain technology areas. It is important for USPTO to be attentive to the potential effects that such procedures may have on timeliness. Moreover, sharing these procedures with patent examiners as they are developed can improve examination without causing delays.

In addition, first-action pendency in trademark examination remains well above historical levels. Pendency at this level affects applicants' ability to plan and make timely business decisions.

First-action pendency: The number of months between the application filing and the examiner's first action.

Although the application growth rate has slowed, USPTO is challenged to reduce pendency to levels consistent with stakeholder needs while maintaining examination quality.

Preventing Fraud and Preserving Patent and Trademark Application Integrity

The integrity of patent and trademark examination and trial proceedings are important to reliable intellectual property rights and the economic health of the United States. In recent years, USPTO has seen significant increases in fraudulent trademark filings and has taken steps to address improper conduct. Its challenge is to ensure that its actions are coordinated, effective, and modified as needed.

Other reports have also identified areas of concern regarding the transparency of USPTO's operations. For example, a 2022 report by GAO found that the Patent Trial and Appeal Board was not clear about the factors it considered when denying requests for patent trials and how it handled multiple petitions filed to challenge the same patent. The GAO report found that USPTO's review and oversight of judges' work lacked transparency and affected judges' ability to operate without influence.²³ According to GAO's website, the report's recommendations remain open.

In addition, the most recent edition of USPTO's *Manual of Patent Examining Procedure*, published in February 2023, contained changes that had become effective 7 months before, in July 2022. Communicating procedural changes promptly can help increase transparency, reduce time and expense for applicants, and allow examiners to work more efficiently.

Ensuring Quality Population Data

The Census Bureau carries out the decennial census as well as other population surveys that measure changing U.S. demographic and economic conditions.

Decennial census: Constitutionally required count of the U.S. population, conducted every 10 years.

Since the results of these efforts are used in making political, economic, and social policy decisions, the bureau's data must be accurate. However, the bureau continues to face lower response rates, which can reduce the quality of its data.

The bureau is coping with the lower response rates through various methods, such as using proxy data or administrative records to gather data on nonresponsive households. It must, however, still find ways to carry out its operations and maintain data quality for the many products used by its stakeholders.

Data Collection: Addressing Issues That May Affect Data Quality

The bureau has several response collection methods for the decennial census and other surveys. Response options include Internet self-response, mail, telephone, or in-person follow-up (in which Census staff visit households and record responses in person).

For households that do not respond, the bureau may obtain data from proxies, such as neighbors. If any data gaps remain at that point, the bureau may impute data from its own administrative records or records obtained from other government agencies. But the bureau is still contending with other

operational problems that can also lead to lower data quality.

For example, in 2022, we reported that college and university students at off-campus addresses were likely undercounted despite outreach efforts, a significant number of follow-up counts were completed using proxies, and the 2020 census's quality assurance plan was improperly executed, all of which may have adversely affected the decennial's data quality.²⁴ The bureau has responded that it would evaluate the lessons from our report as it plans for the 2030 census.

GAO has also highlighted potential adverse impacts to 2020 census data quality:

- In June 2020,²⁵ GAO noted that the bureau extended the period for self-response because of COVID-19 but expressed concern about compressed timeframes for data collection processing affecting data quality.
- In August 2020,²⁶ GAO found the bureau faced higher-than-expected staff attrition rates that required it to improve staff onboarding to maintain adequate levels to carry out operations.
- In a December 2020 report,²⁷ issued after the 2020 census's field operations were completed, GAO cautioned that delayed operations, stemming in part from the impact of the COVID-19 pandemic, and compressed operational timeframes might have affected the bureau's ability to deliver quality data results.

Reimbursable Surveys: Improving Data Quality

In 2023 we completed an audit of the bureau's demographic programs directorate, which carries out reimbursable surveys on behalf of other U.S. government agencies. Our objective was to determine whether quality metrics were

met and quality assurance processes were carried out as intended. Our audit assessed three major surveys.²⁸ We found that data collection targets were not met, with declining response rates affecting each one, and that quality assurance processes were not always followed.

For one survey, the Current Population Survey, we found issues including inadequate investigation of discrepancies and potential falsification of responses by Census employees. We made 15 recommendations to improve the bureau's data quality assurance processes. In its response to the report, the bureau stated that it would evaluate strategies to increase response rates, work to ensure reinterviews are completed on time, improve timeliness and documentation of falsification investigations, and evaluate the impact of falsified cases on survey estimates. While the bureau's action plan addresses our 15 recommendations, 10 remain open.

Continuous Improvements: Modernizing Data Collection and Decennial Census Processes

The bureau is working on several initiatives to modernize its data collection, storage,

processing, and dissemination. One is to create a single enterprise-wide IT platform to automate survey and census data collection, which will be critical for the upcoming 2030 decennial.

Another is researching the use of administrative records to help produce a more complete decennial census count. The bureau will need to use administrative records to mitigate nonresponses and improve operations to ensure data is collected accurately.

Finally, we reported in 2024 on a program designed in part to inform research and testing for the 2030 census.²⁹ We found that studies* were not completed in time to formally inform the 2030 research and testing agenda and that the bureau did not prioritize the investigation of a potentially significant innovation. The bureau responded that it would work to publicly release studies by their target dates, establish a centralized repository and document a process for storing lessons learned and recommendations to ensure decision makers have access to this information in the future, and prioritize studies that benefit research and testing.

* The term "studies" encompasses program activities comprising mostly (1) operational assessments that compared operational variances between planned and actual activities, (2) evaluations that described the effectiveness of census operations and processes, and (3) experiments that were carried out during the 2020 census with the aim of informing 2030 census research.

Section 3: Managing Spending

In recent years, the Department has been at the forefront of efforts to strengthen the American economy and global competitiveness. This has led to many new programs and initiatives for the Department to manage. As the Department's funding for these programs and initiatives has grown, so has its ongoing challenge of ensuring the proper oversight and management of contracts, grants, and financial assistance awards. The Department must manage many high-dollar award programs and procurements while ensuring that it spends taxpayer dollars prudently and safeguards programs from fraud, waste, and abuse.

Managing and overseeing major programs, like NIST's manufacturing partnership program, NTIA's broadband programs, CHIPS Act programs, and FirstNet Authority's management of the Nationwide Public Safety Broadband Network, are some of the spending-related challenges the Department has to meet to carry out its wide-ranging mission.

Strengthening Oversight in Response to Dramatic Growth

Safeguarding the funds obligated for the Department's complex programs and initiatives is a major ongoing challenge.

Protecting these funds will require strong management and oversight, which in turn depend on the Department's ability to hire and retain a skilled grants and acquisitions workforce and to maintain a proactive approach to preventing and detecting fraud and ensuring the accountability of recipients.

Grants and Contracts: Strengthening Monitoring and Oversight

The Department's grant funding continues to grow. In FY 2023, approximately \$5.6 billion was obligated for grants. The Department has surpassed that amount in FY 2024, obligating approximately \$18 billion for initiatives such as providing broadband infrastructure and increasing resilience to climate change.

Going forward, the Department plans to significantly increase investments in new and ongoing programs. Some key increases planned for FY 2025 are listed below.

\$4.1 billion

For economic development programs

\$2.8 billion

To promote digital equity

\$300 million

In semiconductor manufacturing R&D

\$223.4 million

To strengthen export controls

\$47.7 million

To safeguard, regulate, and promote AI

The Department must continue to strengthen its grants administration and oversight and ensure compliance with laws and regulations. Thorough performance monitoring and documentation help ensure that the Department and bureaus provide effective oversight and comply with all applicable regulations and that grant recipients are fiscally responsible with federal funds.

In addition to grants, the Department obligated approximately \$5 billion for contracts in FY 2023. In FY 2024, it has obligated \$3.7 billion; in FY 2025, contracting for goods and services is likely to increase as the Department establishes resilient supply chains to strengthen our national security and economic prosperity and create high-paying American jobs. The Department has also stated that it plans to invest over \$400 million in fundamental research infrastructure at NIST, NOAA, and NTIA.

With billions of tax dollars spent each year in government contracting, federal acquisitions must be managed effectively, efficiently, and accountably. As contractors deliver goods and services to help the Department perform its mission, strong internal controls must be in

place to provide the best value for taxpayers' resources.

Our recent audit work, however, has shown that the Department needs to improve its contractor monitoring and acquisition oversight. Two examples are below.

Managing and monitoring contractor performance at the Census Bureau. A May 2024 audit concluded that the bureau did not provide adequate oversight over four task orders, worth \$436.5 million, of the 2020 advertising contract and thus has no assurance the contractor complied with contractual requirements. We questioned \$363 million in payments for media services as unsupported costs because documentation for the services was not maintained as required.

Strengthening acquisition oversight at USPTO. USPTO's biennial budget for acquisitions exceeds \$1.8 billion. By statute, USPTO is not required to follow certain federal regulations for competition in contracting; therefore, USPTO needs strong oversight to reduce its risks of paying for unneeded services and paying more while receiving less. In recent audits, we reported that USPTO needs to strengthen oversight of its contract for patent data capture services, better define how to use its acquisition guidelines, and strengthen its acquisition management.

Grants and Acquisitions Workforce Management: Hiring, Training, and Retaining a Skilled Workforce

Hiring and retaining skilled workers has long been a challenge for the Department. In its FY 2025 budget, the Department plans to request at least an additional \$1.3 billion and 1,064 positions to fund and operate a variety of programs.

A key part of this hiring will be to support and manage the increased funding for grants,

contracts, and financial assistance. A skilled acquisition workforce will be essential as the Department continues with the high-dollar investments we discussed in sections 1 and 2 of this report, including implementation of the Grants Enterprise Management Solution and Business Application Systems, ship and aviation recapitalization, and next-generation satellite systems.

The Department has several human capital goals through FY 2025. These include maximizing available incentives, exploring new strategies to recruit and retain acquisition professionals, and researching state-of-the-art technology to complete tasks faster (such as predictive analysis and artificial intelligence).

The Department's Office of Acquisition Management also shared with us several accomplishments in managing and strengthening its acquisition workforce. These included providing employee training, continuing to develop its acquisition innovation lab to provide an environment to explore new ideas and share lessons learned, and developing a program management tool to identify talent within the Department.

Notwithstanding these efforts, 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 Office of Acquisition Management's *FY 2022 Acquisition Human Capital Report* have cited several challenges that show the Department's difficulties in attracting experienced staff, hiring and training them, and providing enough incentives and advancement opportunities to retain them.

Fraud Management: Mitigating Fraud and Improving Accountability

All federal programs and operations are at risk of fraud.³⁰ A 2024 GAO report has estimated direct annual financial losses to the federal government from fraud to be between approximately \$233 billion and \$521 billion.³¹ With the historic funding amounts the Department has received in recent years, it will need robust processes in place to prevent, detect, and respond to fraud.³²

\$233 billion–\$521 billion

Estimated annual fraud losses to the government (GAO, 2024)

In light of these concerns, managing fraud risk should be a key part of the Department's program implementation and oversight. Effective fraud risk management helps to ensure that federal programs' services fulfill their intended purpose, funds are spent effectively, and assets are safeguarded.³³ We summarize several elements of an effective fraud management program below.

Requiring accurate data from recipients.

GAO and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) have both cited the benefits of data analytic tools and techniques for effective fraud prevention and detection. A 2021 CIGIE report noted that using data analytics throughout a grant's lifecycle can provide greater visibility and insight into the use of federal funds and result in greater accountability.³⁴ As the Office of Management and Budget (OMB) has pointed out, financial award and subaward data must be accurate and of high quality to provide transparency in how federal funding is spent.³⁵

One way to help ensure the quality of grant data is to require grantees to certify the accuracy and truthfulness of the information they give the Department in applications, reports, and support for expenditures.

Robust certifications can also contribute to effective civil and criminal grant fraud enforcement³⁶—which, in turn, improves accountability.

Ensuring accountability for subrecipient performance. Accurate data is even more important at the subrecipient level, which is particularly vulnerable to fraud. OMB has stated that prime recipients are responsible for reporting subaward data and that agencies must hold recipients accountable for this reporting.³⁷ The Department accordingly should ensure that recipients of funding are meeting their subrecipient reporting requirements.

Collaborating and coordinating with OIG. According to GAO, another important component of effective fraud risk management is for federal agencies to collaborate and coordinate with their OIGs.³⁸ OMB notes that agencies' leadership and OIGs share the responsibility of promoting economy, efficiency, and effectiveness in the agencies' programs and preventing and detecting fraud and abuse.³⁹

The Department is required to report to us on possible fraud and other criminal matters such as a false claim by a grantee, contractor, or financial assistance recipient.⁴⁰ Timely reporting of these issues helps prevent and mitigate fraud in the Department's programs. Active engagement with us on fraud risk management, to include providing award data for our analysis, is one important aspect of these prevention and mitigation efforts.

Strengthening Oversight of the Hollings MEP Program

NIST's Hollings Manufacturing Extension Partnership (MEP) is a national network aimed at enhancing productivity and technological performance of U.S. manufacturing.⁴¹ NIST enters into cooperative agreements with state, university, and nonprofit organizations, which operate 51 MEP centers (one in each state and in Puerto Rico) to help U.S. manufacturers improve production processes, upgrade technological capabilities, facilitate production innovation, and more.

MEP's appropriations have steadily increased, and funding is authorized to surge over the next 3 years to \$550 million in FY 2027. However, NIST's inadequate oversight has placed the program, and the taxpayer money that funds it, at risk. In 2023, we reported that NIST's inadequate oversight of MEP led to inefficient use of financial resources related to the centers in our review:⁴²

- NIST did not ensure that centers used all funds to further MEP's mission. Instead, NIST allowed centers to keep and use millions of dollars for their own purposes with no accountability to the federal government or taxpayers.
- NIST did not review the reasonableness of centers' executive salaries, resulting in excessive center personnel costs.
- Centers did not meet their award requirement to disclose potential conflicts of interest to NIST. This raises concerns about how they use award funds and increases the risk of fraud, waste, and abuse in the program.

As a result of our findings, we identified nearly \$6.9 million in total funds that could be put to better use.

Since issuing that report, we continue to find instances where NIST allowed centers to retain significant financial resources for their own purposes and where award terms were breached.

Most recently, our September 2024 evaluation found that NIST publicly reported unreliable economic impact data, including 48 percent of the FY 2022 total sales for the seven centers in our review.⁴³ NIST also overstated MEP's return on investment from FYs 2020 through 2023—notably, by 34 percent in FY 2020.

NIST reports this data in many contexts, ranging from its public-facing website to budget justifications. It is accordingly key information for many potential decision makers, including as NIST's primary means of evaluating centers' performance for continued federal funding. However, NIST's reliance on this data to evaluate centers may have caused it to provide federal funds to centers that overstated their performance.

Inefficient use of financial resources and unreliable, overstated economic impact data increase the risk of fraud, waste, and abuse throughout the program. We will continue to monitor the program and review its progress in addressing this challenge.

Managing Major Broadband Grant Programs

Through NTIA, the Department is responsible for administration and oversight of six grant programs worth a total of \$49.8 billion, with the shared goal of bringing broadband access to every American.⁴⁴ The combination of standing up new programs and increasing access to broadband for all Americans continues to be a national challenge.

Recent work by our office and GAO has identified weaknesses in NTIA's processes for managing broadband grants. These challenges include ensuring proper allocation and awarding of funds and identifying and overcoming stakeholders' difficulties when implementing broadband programs.

Broadband Infrastructure: Ensuring Proper Fund Allocations and Awards

NTIA must ensure that grant funds are properly allocated, awarded, and used. Recent reports have identified challenges in ensuring that broadband infrastructure funds are awarded only for eligible proposed service areas. If these challenges are not addressed, they could impact NTIA's ability to reduce fraud risk and provide assurance that awards went to applicants that needed them.

A recent GAO report found that NTIA did not fully develop measurable performance goals for some of its broadband grant programs.⁴⁵ Additionally, our April 2024 audit found NTIA did not adequately design and implement the award process to ensure Tribal Broadband Connectivity Program funds were awarded only for eligible proposed service areas.⁴⁶ As a result, NTIA may have made awards that created overbuilding of broadband infrastructure and reduced the amount of funding available to tribes that needed the funds. On August 21, 2024, we approved NTIA's action plan to address our April 2024 audit findings and the related recommendations, and deemed the recommendations resolved.

As NTIA allocates funding for the remaining programs, addressing weaknesses in grant award processes is essential. Developing and measuring performance goals is also needed to ensure grant funds are allocated, awarded, and spent appropriately.

Broadband Deployment: Overcoming Stakeholders' Challenges

In FY 2022, the Infrastructure Investment and Jobs Act tasked NTIA with administering grants for four of the six broadband programs. The programs are intended to expand broadband use in America, laying the groundwork for sustainable economic growth, better education, public safety, and healthcare.

In February 2024, we issued a management alert on challenges facing industry stakeholders that could significantly delay broadband deployment and negatively affect the goal of closing the digital divide.⁴⁷ GAO has also reported on industry challenges affecting middle mile network coverage (*middle mile* refers to connecting a major network with local networks) and access related to the costs of serving low-population areas, deploying infrastructure across challenging terrain, and obtaining permits.⁴⁸

Mitigating these challenges is necessary to close the digital divide and deploy broadband service to unserved and underserved communities. The challenges could impact stakeholders' ability to successfully deploy broadband, discourage technology providers from applying for grants, decrease competition, encourage wasteful spending to connect locations with existing broadband access, and increase deployment cost.

An emerging challenge lies in developing a workforce that can perform the complex technical work involved in broadband implementation. Building long-term opportunities for career advancement is key to developing a sustainable broadband workforce; however, the industry faces challenges in attracting, training, and retaining employees:

- In our February 2024 management alert, we noted recruiting challenges for trained and

experienced workers, a lack of messaging to promote telecommunications as a viable career field, and a lack of standardized broadband workforce training.

- In its report on middle mile coverage, GAO noted challenges finding labor to support the increased demand for broadband deployment for middle mile networks.

The Department has begun taking steps to address this issue:

- The Department continues to work with states and territories to prepare a workforce development plan to address the workforce demand for the Broadband Equity Accessibility and Deployment (BEAD) Program.
- NTIA released workforce planning guidance to support states and territories developing their workforces for grant implementation as well as designing workforce plans and standards for subgrantees.
- NTIA created a workforce development webpage with additional resources and case studies highlighting existing development programs.

The Department has also made progress in addressing some of the other challenges we identified in our FY 2024 *Top Management Challenges* report, including mitigating regulatory challenges for supply chain issues and developing initiatives to streamline the permitting process:

- NTIA issued Build America Buy America waivers for the Middle Mile Grant Program⁴⁹ and BEAD,⁵⁰ allowing providers to purchase some items from foreign sources to fulfill their obligations when American products are unavailable.
- NTIA launched the Permitting and Environmental Information Application in March 2024 to help grant recipients and others deploying infrastructure identify

permit requirements and avoid issues when connecting high-speed Internet service. NTIA continues to work on new initiatives to provide streamlined and efficient regulatory frameworks to mitigate the lengthy permitting process.

Managing and Overseeing CHIPS Funding

In 2022, Congress passed the CHIPS and Science Act⁵¹ to promote long-term growth in domestic semiconductor manufacturing and research in support of national and economic security.

The CHIPS Act of 2022 authorizes direct funding to support semiconductor research and development, innovation, and manufacturing.⁵² The CHIPS Act also provided \$1.5 billion to the Public Wireless Supply Chain Innovation Fund for grants to promote and deploy 5G technology while increasing innovation and competition.

These initiatives represent major priorities of the administration. Managing the programs so they meet their goals is an ongoing challenge for the Department.

CHIPS: An Unparalleled Investment in the U.S. Semiconductor Industry

NIST must award and manage \$50 billion in CHIPS Act direct funding and up to \$75 billion in loans and loan guarantees. The bureau plays a pivotal role in the attempt to bring semiconductor development and manufacturing back to the United States.

The two offices put in place to implement CHIPS, the Program Office and the Research and Development Office, have begun notifying potential CHIPS applicants about funding opportunities. As of September 2024, the Program Office has announced 16 nonbinding

preliminary funding agreements valued at over \$32 billion and up to \$28.8 billion in loans, as well as one official award worth up to \$123 million.

The scale and complexity of the program increases the risk of operational inefficiencies and compliance issues. If recipients of CHIPS Act funds mismanage them, the Department could fail to achieve the legislation's goals. Moreover, failure to implement adequate internal controls and oversight could lead to errors, fraud, waste, and abuse.

CHIPS must have the policies and people in place to provide effective oversight of all funding. However, when we reviewed CHIPS workforce management,⁵³ we found that although CHIPS had surpassed its hiring goals, it had not developed a comprehensive workforce management plan. Workforce planning, as outlined by the Office of Personnel Management,⁵⁴ serves as the foundation for effective human capital management, ensuring that agencies have personnel with the skills needed to accomplish the mission and meet organizational goals and objectives.

As of March 29, 2024, the CHIPS program office decided to delay funding for the construction, modernization, or expansion of semiconductor research and development facilities in the United States. According to the program office, this was due to overwhelming demand for funding and changes in the FY 2024 appropriations law, which reprogrammed \$3.5 billion of the program office's incentive program to create secure facilities.

The Innovation Fund: CHIPS Act Funding to Support Advancements in 5G Technology

Authorized in 2021, the Innovation Fund aims to support the United States' leading position in the telecommunications ecosystem, reduce costs, enhance competition, and strengthen

the nation's telecommunications supply chain.⁵⁵ NTIA is administering Innovation Fund grants for the Department.

NTIA met its August 8, 2023, statutory deadline for awarding the first Innovation Fund grants. As we explained in our FY 2024 *Top Management Challenges* report, NTIA had a very short time—about 2 months—to review applications and award grants. It received 125 applications and awarded three grants, totaling approximately \$5.5 million, in August 2023.

As of May 2024, NTIA has awarded 17 grants, totaling \$140.5 million, and issued its second notice of funding opportunity with up to \$420 million to be granted on a rolling basis. NTIA plans to announce additional funding opportunities later in the year.

Because this is a new program, NTIA's challenge for FY 2025 is to establish and implement a comprehensive control framework to ensure that funds are granted to eligible applicants and used according to the Innovation Fund's objectives.

The CHIPS Act also appropriated \$2 million each fiscal year until 2032 to our office for oversight. As part of this, we are required to audit six Innovation Fund areas within 4 years after funds are disbursed to determine whether grants were awarded to eligible applicants and funds were used as the program intended. We are evaluating the program's implementation as the first of our planned projects.

Overseeing the NPSBN Program

NTIA's First Responder Network Authority manages the building, deployment, and

operation of the Nationwide Public Safety Broadband Network (NPSBN) dedicated to first responders. Since 2017, FirstNet Authority has managed a 25-year, \$6.5 billion contract with AT&T for the network's construction and operation.[†]

The NPSBN contract is a high-profile, mission-critical program that warrants particular management attention. Appropriate contract administration is essential to the NPSBN's success, but our most recent audit reports show that FirstNet Authority has missed many opportunities to fully assess AT&T's performance and hold it accountable. As a result, FirstNet Authority cannot ensure that the NPSBN's goals are being met or that AT&T is meeting contractual terms or the needs of its customers in the public safety community.

We identified oversight of the contract's task orders as a top management challenge in FYs 2023 and 2024.⁵⁶ Deficiencies in FirstNet Authority's contract administration, including weaknesses in contract oversight and inconsistent adherence to federal and departmental regulations, are ongoing challenges.

Several of our recent reports have also noted that the contract's performance assessment guidelines are insufficient.⁵⁷ As a result, FirstNet Authority does not always have the tools to adequately assess AT&T's performance.

The NPSBN contract states that public safety adoption and use of the network are primary FirstNet Authority programmatic objectives and that it is important for AT&T to maintain and increase public safety adoption throughout the life of the contract. At its June 24, 2024, board meeting,⁵⁸ FirstNet Authority reported the following progress:

[†] AT&T pays lease fees to FirstNet Authority for the use of NPSBN capacity. Of the \$18 billion FirstNet Authority will receive from AT&T over 25 years, approximately \$15 billion is expected to be used for reinvestments.

- More than 28,000 public safety agencies were using the NPSBN via more than 6 million device connections
- The NPSBN maintained an inventory of more than 180 dedicated deployable network assets, such as flying cells on wheels, to provide connectivity when normal network access is not available
- More than 210 unique applications were listed in the *FirstNet App Catalog*
- AT&T had deployed the initial coverage buildout for Band 14 (the dedicated broadband spectrum for public safety)

However, as we reported in June 2024, FirstNet Authority has not provided the oversight needed to accurately verify eligible first responders' adoption and use of the NPSBN. Inadequate oversight may also allow ineligible users and unapproved devices on the network, which could impact first responders' use of the network. Without an effective verification process, FirstNet Authority may not identify issues that could negatively impact the first responders who rely on the network to effectively manage emergencies.

FirstNet Authority has submitted action plans to address our audit findings from FY 2023 and is in the process of submitting plans to address our FY 2024 findings. However, continued oversight is needed to ensure that the NPSBN's reported successes are substantiated and FirstNet Authority's action plans are effectively implemented.

Until FirstNet Authority puts in place sufficient surveillance plans and appropriate performance measures for the contract, it will continue to put the NPSBN program—and the billions of dollars that fund it—at risk.

Overseeing NIST Facility Improvement Project Contracts

NIST's scientific research affects our national security and contributes to innovative manufacturing that helps drive the U.S. economy. In FY 2025, NIST continues to face the challenge of effectively managing funding for the construction and maintenance of its facilities, including expansion and renovation projects, as it takes a central role in promoting U.S. innovation and technological competitiveness.

Several organizations[‡] have raised concerns about the poor state of NIST's facilities.⁵⁹ One study by the National Academies of Sciences, Engineering, and Medicine (NASEM) concluded that NIST's facilities, which date back to the 1950s, are outmoded and dilapidated and that its research facilities and laboratories overwhelmingly fail to meet the Department's own standards for acceptable building conditions.⁶⁰ The NASEM study also concluded that the inadequacy of NIST's facilities threatens its mission performance by causing substantive delays in key national security deliverables, scientific research, and services to U.S. industry customers.⁶¹

Outdated facilities create safety and health concerns for NIST's workforce and have led to millions of dollars in equipment damage. Laboratories in particular suffer from a variety of issues with unreliable climate control, plumbing, and power, which contribute to productivity losses of up to 40 percent for NIST researchers.

Historically, NIST has not received consistent, significant funding to execute multiple large construction and maintenance projects.

[‡] One organization, the Visiting Committee on Advanced Technology of the National Institute of Standards and Technology, reviews and makes recommendations on general policy for NIST's organization, budget, and programs. The committee submits an annual report to the Secretary of Commerce for submission to Congress. A nongovernmental organization, the National Academies of Sciences, Engineering, and Medicine, issued an extensive study in 2023 on NIST's facility conditions.

Further, the facilities' issues will take years to rectify, and current funding may not be sufficient. To prioritize its construction and maintenance projects, NIST will need a plan that considers (among other things) national security interests, critical emerging technologies, and cost-benefit analyses.

NIST will face significant pressure to quickly address its facilities' condition, but it must practice prudent financial management if it is to make the most of any funding it receives. NIST will need to ensure that construction contracts are awarded fairly and in compliance with applicable requirements. It must also

closely monitor contracts 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 has developed a coordinated recovery plan to fund major modernizations while improving its facilities' conditions and functionality. However, this plan is dependent on sustained, long-term funding from Congress and may need to be updated. As NIST begins implementing the plan, our office will monitor and review its progress in addressing this challenge.

Appendix:

Relevant OIG Reports and Ongoing Projects

Section 1: Modernizing Technology and Systems

Cybersecurity and IT Security

[*Fundamental Deficiencies in OS' Cybersecurity Incident Response Program Increase the Risk of Cyberattacks*](#) (OIG-23-017-I)

[*Security Weaknesses in the Department's Mission-Critical High Value IT Assets Leave the Assets Vulnerable to Cyberattacks*](#) (OIG-23-030-A)

[*The Department Needs to Fully Implement Strong Multifactor Authentication for Its High Value Assets to Protect Them from Cyberattacks*](#) (OIG-24-009-A)

ONGOING PROJECT

- [Audit of the Department's Enterprise Continuous Diagnostics and Mitigation Program](#)

Modernizing Systems and Programs

[*Management Alert: BAS Program's Focus on Technology May Overlook Risks Related to Business Processes*](#) (OIG-21-023-M)

[*The Success of NOAA's Next-Generation Satellite System Architecture Depends on Sound Requirements Management Practices*](#) (OIG-22-022-A)

[*The BAS Program Needs to Increase Attention to Business Process Reengineering and Improve Program Management Practices*](#) (OIG-22-025-A)

[*Space Weather Follow-On \(SWFO\) Program: Rideshare Schedule Presents Challenges and Lack of Backup Option Warrants NOAA Attention*](#) (OIG-23-015-A)

[*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)

[*The Department Needs to Improve Oversight to Ensure the Success of Its Financial System Modernization*](#) (OIG-24-014-A)

[*A Lack of Program Management Controls and Attention to IT Security Threaten the Success of NOAA's Effort to Implement a Cloud-Based Common Ground System*](#) (OIG-24-034-A)

ONGOING PROJECTS

- [Audit of GEMS Implementation](#)
- [Audit of NOAA's GeoXO Program Implementation](#)

AI and Emerging Technologies

[USPTO Needs to Improve Its Cost Estimating, Scheduling and Agile Practices to Timely Retire Legacy Systems](#) (OIG-22-026-A)

[Top Management Challenges for FY 2024](#) (OIG-24-002)

ONGOING PROJECT

- [Audit of USPTO's Governance of Its AI Tools](#)

Section 2: Providing Core Services and Data

Secure, Fair Trade

[Lack of Defined Processes and Procedures Impede Efforts to Monitor End Use Check Performance](#) (OIG-20-19-A)

[ITA Did Not Effectively Resolve Foreign Trade Barriers](#) (OIG-24-004-A)

[BIS' Export License Approval Process Reduces Risk of Threats from China's Military-Civilian Fusion Strategy, but BIS Should Take Additional Steps to Mitigate Risks of Unauthorized Technology Release to China's Military](#) (OIG-24-036-A)

ONGOING PROJECTS

- [Audit of BIS's Enforcement of Russia and Belarus Export Controls](#)

NOAA's Operations and Services

[NWS's Verification System for Severe and Hazardous Weather Forecasting Needs Modernization Inspection](#) (IPE-9255)

[NOAA's Office of Marine and Aviation Operations Needs to Improve the Planning and Governing of Its Ship Fleet Recapitalization Effort](#) (OIG-20-006-A)

[OMAO Must Define and Implement a Disciplined Requirements Management Process to Ensure Future Acquisitions Meet User Needs](#) (OIG-21-027-I)

[Space Weather Follow-On \(SWFO\) Program: Rideshare Schedule Presents Challenges and Lack of Backup Option Warrants NOAA Attention](#) (OIG-23-015-A)

[Satellite Integration and Test Phase Improvements Are Needed to Ensure the Success of Future Polar Weather Satellite Missions](#) (OIG-23-027-A)

[Management Alert: NOAA Must Take Action to Address Significant Ship Fleet Recapitalization Risks](#) (OIG-24-016-I)

[NOAA's Office of Space Commerce Efforts to Provide Space Situational Awareness Services Have Been Delayed and Need a Realistic Schedule](#) (OIG-24-031-A)

ONGOING PROJECTS

- [Evaluation of NWS Tornado Forecasting and Warning Performance](#)
- [Audit of NWS Hurricane Forecasting and Warning Performance](#)
- [Assessing Progress of NOAA's Hurricane Hunter Replacement](#)

Intellectual Property and Innovation

[USPTO Has Opportunities to Improve Its Internal Controls and Oversight Related to PTA and PTE Calculations](#) (OIG-21-030-I)

[USPTO Should Improve Controls over Examination of Trademark Filings to Enhance the Integrity of the Trademark Register](#) (OIG-21-033-A)

[USPTO Has Opportunities to Improve its Patent Examination Process and to Advance Patent Decision-Making](#) (OIG-22-010-I)

[USPTO Needs to Improve Oversight and Implementation of Patent Classification and Routing Process](#) (OIG-23-026-A)

[The Department Needs to Strengthen Its Ethics Oversight for USPTO Patent Examiners](#) (OIG-24-013-I)

ONGOING PROJECTS

- [Audit of USPTO's Management of Trademark Pendency](#)
- [Audit of USPTO's Quality Reviews of Continuing Patent Applications](#)

Ensuring Quality Population Data

[The Census Bureau Needs to Improve its Performance Management Processes and Quality Control Program for the Reimbursable Surveys Program](#) (OIG-23-025-A)

[Independent Evaluation of the 2020 Decennial Census Evaluation and Experiments Operation](#) (OIG-24-011-I)

Section 3: Managing Spending

Strengthening Oversight in Response to Dramatic Growth

[2020 Census: The Bureau Can Improve Oversight of Time-and-Materials Delivery Orders on the Integrated Communications Contract](#) (OIG-20-025-A)

[USPTO Should Strengthen Its Planning and Oversight of Patent Data Capture Contracts to Manage Risks and Prevent Unnecessary Costs](#) (OIG-22-028-A)

[EDA Generally Maintained Grant Award Files During the COVID-19 Pandemic](#) (OIG-23-029-I)

[NTIA Took the Necessary Steps to Implement the Requirements for Awarding Funds Under the Consolidated Appropriations Act, 2021](#) (OIG-23-018-I)

[EDA Implemented and Followed the Requirements for Awarding and Disbursing CARES Act Funding Through the Revolving Loan Fund Program](#) (OIG-23-021-I)

[EDA Generally Monitored Grants Awarded Under the FY 2019 EDA Disaster Supplemental Notice of Funding Opportunity](#) (OIG-24-005-A)

[USPTO Must Improve Acquisition Planning to Ensure Efficient and Competitive Procurements](#) (OIG-24-008-A)

[The Census Bureau Did Not Effectively Manage and Monitor Contractor Performance for Paid Advertising in the 2020 Census Integrated Communications Contract](#) (OIG-24-021-A)

[The Puerto Rico Department of Natural and Environmental Resources Needs to Fully Comply with Procurement Regulations When Executing NOAA Awards](#) (OIG-24-028-A)

[Independent Program Evaluation of NIST Pandemic Relief Program](#) (OIG-24-017-I)

[Independent Program Evaluation of NOAA Fisheries Pandemic Relief Program](#) (OIG-24-018-I)

ONGOING PROJECTS

- [Audit of Cares Act Grant Recipients Through EDA's Revolving Loan Fund Program](#)
- [Costs Claimed through Disaster and Pandemic Relief Funds](#)
- [Audit of the MBDA Business Center Program](#)

NIST's MEP Oversight

[NIST Must Improve Monitoring of MEP to Prevent Waste of Financial Resources](#) (OIG-23-014-I)

[NIST Overstated MEP's Economic Impacts to Congress and Other Stakeholders](#) (OIG-24-037-I)

ONGOING PROJECTS

- [Audit of NIST Cooperative Agreements with Ohio Department of Development](#)

Broadband Grant Programs

[Management Alert: NTIA's Reliance on Self-Certifications Increased Fraud Risk for the Tribal Broadband Connectivity Program](#) (OIG-23-022-M)

[Management Alert: Challenges Industry Stakeholders Face with Broadband Deployment](#) (OIG-24-015-M)

[NTIA's Award Processes Leave Tribal Broadband Grants Vulnerable to Fraud and Duplication](#)
(OIG-24-019-A)

ONGOING PROJECT

- [Evaluation of Broadband Deployment Challenges](#)

CHIPS and Innovation Fund

[NIST Surpassed Hiring Goals for CHIPS But Did Not Develop a Comprehensive Workforce Plan](#)
(OIG-24-023-I)

ONGOING PROJECTS

- [Evaluation of NTIA's Implementation of the Public Wireless Supply Chain Innovation Fund](#)
- [Status Report on the Department of Commerce's CHIPS Act Programs](#)

NPSBN Program Oversight

[FirstNet Authority Failed to Provide Adequate Contract Oversight for its Initial Two Reinvestment Task Orders](#) (OIG-23-012-A)

[Management Alert: The NPSBN Band 14 Signal Strength Does Not Consistently Provide Adequate Band 14 Service for First Responders Final Memorandum](#) (OIG-24-022-M)

[FirstNet Authority Did Not Ensure the Nation's First Responders' Needs Were Continuing to Be Met Timely When Modifying Key Objectives of the NPSBN Contract](#) (OIG-24-024-A)

[FirstNet Authority's Lack of NPSBN Contract Oversight for Coverage Puts at Risk First Responders' Ability to Serve the Public Effectively](#) (OIG-24-026-A)

[FirstNet Authority's Lack of Contract Oversight for Device Connection Targets Puts the NPSBN at Risk of Impacting First Responders' Use of the Network](#) (OIG-24-027-A)

[Management Alert: February 2024 FirstNet Authority's Nationwide Public Safety Broadband Network Outage Raised a Significant Risk to the Readiness of First Responders Across the Country](#)
(OIG-24-030-M)

ONGOING PROJECTS

- [Audit of NPSBN Services During Maui Wildfires](#)
- [Audit of the First Responder Network Authority's Oversight of Service Availability for the Nationwide Public Safety Broadband Network](#)

References

- ¹ Executive Office of the President, May 12, 2021. [Executive Order 14028](#): *Improving the Nation’s Cybersecurity*. Washington, DC: Executive Office of the President.
- ² Office of Management and Budget (OMB), January 26, 2022. *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, Memorandum M-22-09, 1. Washington, DC: OMB.
- ³ Department of Commerce Office of Inspector General (OIG). October 12, 2023. *Top Management and Performance Challenges Facing the Department of Commerce in Fiscal Year 2024*, OIG-24-002. Washington, DC: DOC OIG.
- ⁴ OIG, January 22, 2024. *The Department Needs to Fully Implement Strong Multifactor Authentication for Its High Value Assets to Protect Them from Cyberattacks*, OIG-24-009-A. Washington, DC: DOC OIG.
- ⁵ 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.
- ⁶ 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.
- ⁷ GAO, 2023. *High Risk List*, “[Improving the Management of IT Acquisitions and Operations](#).”
- ⁸ (1) OIG, July 7, 2022. *The BAS Program Needs to Increase Attention to Business Process Reengineering and Improve Program Management Practices*, OIG-22-025-A. Washington, DC: DOC OIG. (2) OIG, February 22, 2024. *The Department Needs to Improve Oversight to Ensure the Success of Its Financial System Modernization*, OIG-24-014-A. Washington, DC: DOC OIG.
- ⁹ OIG, August 27, 2024. *A Lack of Program Management Controls and Attention to IT Security Threaten the Success of NOAA’s Effort to Implement a Cloud-Based Common Ground System*, OIG-24-034-A. Washington, DC: DOC OIG.
- ¹⁰ [Advanced Weather Interactive Processing System](#) (accessed August 2023).
- ¹¹ 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.
- ¹² (1) Executive Office of the President, December 3, 2020. [Executive Order 13960](#): *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*. Washington, DC: Executive Office of the President. (2) Executive Office of the President, October 30, 2023. [Executive Order 14110](#): *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*. Washington, DC: Executive Office of the President.

- ¹³ (1) NIST, July 2024. *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile*, [NIST AI 600-1](#). Gaithersburg, MD: NIST. This is a companion resource for NIST’s January 2023 *Artificial Intelligence Risk Management Framework* ([NIST AI 100-1](#)) and covers generative AI. (2) NIST, July 2024. *Secure Software Development Practices for Generative AI and Dual-Use Foundation Models*, [NIST SP 800-218A](#). Gaithersburg, MD: NIST. NIST SP 800-218A augments NIST’s February 2022 *Secure Software Development Framework Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities* ([NIST SP 800-218](#)) by adding practices, tasks, recommendations, considerations, notes, and informative references specific to AI model development throughout the software development lifecycle.
- ¹⁴ (1) Executive Office of the President, October 30, 2023. [Executive Order 14110](#): *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*. Washington, DC: Executive Office of the President. (2) [NIST AI 600-1](#).
- ¹⁵ NIST, April 2024. *Reducing Risks Posed by Synthetic Content: An Overview of Technical Approaches to Digital Content Transparency* (initial public draft). [NIST AI 100-4](#). Gaithersburg, MD: NIST.
- ¹⁶ NIST, April 2024. *A Plan for Global Engagement on AI Standards*. [NIST AI 100-5](#). Gaithersburg, MD: NIST.
- ¹⁷ For example, [NIST AI 100-1](#), [NIST SP 800-218](#), and [NIST SP 800-218A](#).
- ¹⁸ OIG, July 20, 2022. *USPTO Needs to Improve Its Cost Estimating, Scheduling and Agile Practices to Timely Retire Legacy Systems*, OIG-22-026-A. Washington, DC: DOC OIG.
- ¹⁹ OIG, September 23, 2024. *BIS’ Export License Approval Process Reduces Risk of Threats from China’s Military-Civilian Fusion Strategy, but Bis Should Take Additional Steps to Mitigate Risks of Unauthorized Technology Release to China’s Military*, OIG-24-036-A, Washington, DC: DOC OIG.
- ²⁰ OIG, March 12, 2024. *NOAA Must Take Action to Address Significant Ship Fleet Recapitalization Risks*, OIG-24-016-I. Washington, DC: DOC OIG.
- ²¹ The definitions for space situational awareness (SSA) and space traffic management (STM) are from the *National Space Traffic Management Policy* (Space Policy Directive-3). The term *STM* has been replaced with *space traffic coordination* in the satellite operation community.
- ²² OIG, July 30, 2024. *NOAA’s Office of Space Commerce Efforts to Provide Space Situational Awareness Services Have Been Delayed and Need a Realistic Schedule*, OIG-24-031-A. Washington, DC: DOC OIG.
- ²³ GAO, December 2022. *Patent Trial and Appeal Board: Increased Transparency Needed in Oversight of Judicial Decision-Making*, GAO-23-105336. Washington, DC: GAO.
- ²⁴ OIG, September 14, 2022. *Lessons Learned from the 2020 Decennial Census*, OIG-22-030. Washington, DC: DOC OIG.
- ²⁵ GAO, June 9, 2020. *2020 Census: COVID-19 Presents Delays and Risks to Census Count*, GAO-20-551R. Washington, DC: GAO.
- ²⁶ GAO, August 27, 2020. *2020 Census: Recent Decision to Compress Census Timeframes Poses Additional Risks to an Accurate Count*, GAO-20-671R. Washington, DC: GAO.

- ²⁷ GAO, December 9, 2020. *2020 Census: The Bureau Concluded Field Work but Uncertainty about Data Quality, Accuracy, and Protection Remains*, GAO-21-206R. Washington, DC: GAO.
- ²⁸ 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.
- ²⁹ OIG, February 5, 2024. *Independent Evaluation of the 2020 Decennial Census Evaluations and Experiments (EAE) Operation*. Washington, DC: DOC OIG.
- ³⁰ GAO, April 2024. *Report to Congressional Committees: Fraud Risk Management*, GAO-24-105833. Washington, DC: GAO.
- ³¹ GAO, April 16, 2024. *Fraud Risk Management*, GAO-24-105833. Washington, DC: GAO.
- ³² (1) NTIA Office of Internet Connectivity and Growth, *2023 Annual Report* (“historic investment”), 6. (2) GAO, July 2015. *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP. Washington, DC: GAO.
- ³³ GAO, July 2015. *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP. Washington, DC: GAO.
- ³⁴ CIGIE, January 2021. *The IG Community’s Joint Efforts to Protect Federal Grants from Fraud, Waste, and Abuse*. Washington, DC: CIGIE.
- ³⁵ OMB, April 4, 2024. *Reducing Burden in the Administration of Federal Financial Assistance*, OMB M-24-11. Washington, DC: OMB.
- ³⁶ CIGIE, January 2021. *The IG Community’s Joint Efforts to Protect Federal Grants from Fraud, Waste, and Abuse*. Washington, DC: CIGIE.
- ³⁷ OMB, April 4, 2024. *Reducing Burden in the Administration of Federal Financial Assistance*, OMB M-24-11. Washington, DC: OMB.
- ³⁸ GAO, July 2015. *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP. Washington, DC: GAO.
- ³⁹ OMB, December 3, 2021. *Promoting Accountability through Cooperation among Agencies and Inspectors General*, OMB M-22-04. Washington, DC: OMB.
- ⁴⁰ Department Administrative Order, 207-10.
- ⁴¹ Omnibus Trade and Competitiveness Act of 1988, Pub. L. No. 100-418, § 5121, 102 Stat. 1107, 1433 (1988).
- ⁴² OIG, March 13, 2023. *NIST Must Improve Monitoring of MEP to Prevent Waste of Financial Resources*, OIG-23-014-I. Washington, DC: DOC OIG.
- ⁴³ OIG, September 25, 2024. *NIST Overstated MEP’s Economic Impacts to Congress and Other Stakeholders*, OIG-24-037-I. Washington, DC: DOC OIG.
- ⁴⁴ OIG, February 6, 2024. *Final Semiannual Status Report on NTIA’s Broadband Programs*, OIG-24-012-I. Washington, DC: DOC OIG, 1.

- ⁴⁵ GAO, October 2023. *Broadband Infrastructure: Middle-Mile Grant Program Lacked Timely Performance Goals and Targeted Measures*, GAO-24-106131. Washington, DC: GAO.
- ⁴⁶ OIG, April 8, 2024. *NTIA's Award Processes Leave Tribal Broadband Grants Vulnerable to Fraud and Duplication*, OIG-24-019-A. Washington, DC: DOC.
- ⁴⁷ OIG, February 29, 2024. Management Alert: *Challenges Industry Stakeholders Face with Broadband Deployment*, OIG-24-015-M. Washington, DC: DOC.
- ⁴⁸ GAO, October 2023. *Broadband Infrastructure: Middle-Mile Grant Program Lacked Timely Performance Goals and Targeted Measures*, GAO-24-106131. Washington, DC: GAO.
- ⁴⁹ Department of Commerce, April 19, 2023. Notice of Final Waiver. [*Limited Applicability Nonavailability Waiver of the Buy America Domestic Content Procurement Preference as Applied to Recipients of Middle Mile Grant Program Awards*](#).
- ⁵⁰ Department of Commerce, February 22, 2024. Notice of Final Waiver. [*Limited General Applicability Nonavailability Waiver of the Buy America Domestic Content Procurement Preference as Applied to Recipients of Broadband Equity, Access, and Deployment Program*](#).
- ⁵¹ CHIPS and Science Act of 2022, Pub. L. No. 117-167, 136 Stat. 1366 (2022).
- ⁵² The CHIPS Act of 2022 (division A of the CHIPS and Science Act) 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.
- ⁵³ OIG, May 20, 2024. *NIST Surpassed Hiring Goals for CHIPS but Did Not Develop a Comprehensive Workforce Plan*, OIG 24-023-I. Washington, DC: DOC OIG.
- ⁵⁴ *OPM Workforce Planning Guide*, November 2022.
- ⁵⁵ NDAA, FY 2021.
- ⁵⁶ OIG-23-001, 32, and OIG-24-002, 39.
- ⁵⁷ (1) 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, 9. (2) OIG, June 5, 2024. *FirstNet Authority's Lack of NPSBN Contract Oversight for Coverage Puts at Risk First Responders' Ability to Serve the Public Effectively*, OIG-24-026-A. Washington, DC: DOC OIG, 10. (3) OIG, June 12, 2024. *FirstNet Authority's Lack of Contract Oversight for Device Connection Targets Puts the NPSBN at Risk of Impacting First Responders' Use of the Network*, OIG-24-027-A. Washington, DC: DOC OIG, 11.
- ⁵⁸ FirstNet Authority, June 24, 2024. [*Combined Board and Committees Meeting*](#). Chicago, IL: FirstNet Authority.
- ⁵⁹ Visiting Committee on Advanced Technology, March 2023. *2022 Annual Report*. Gaithersburg, MD: VCAT.
- ⁶⁰ NASEM, 2023. *Technical Assessment of the Capital Facility Needs of the National Institute of Standards and Technology*. Washington, DC: The National Academies Press.
- ⁶¹ NASEM, 2023. *Capital Facility Needs*, 3.

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