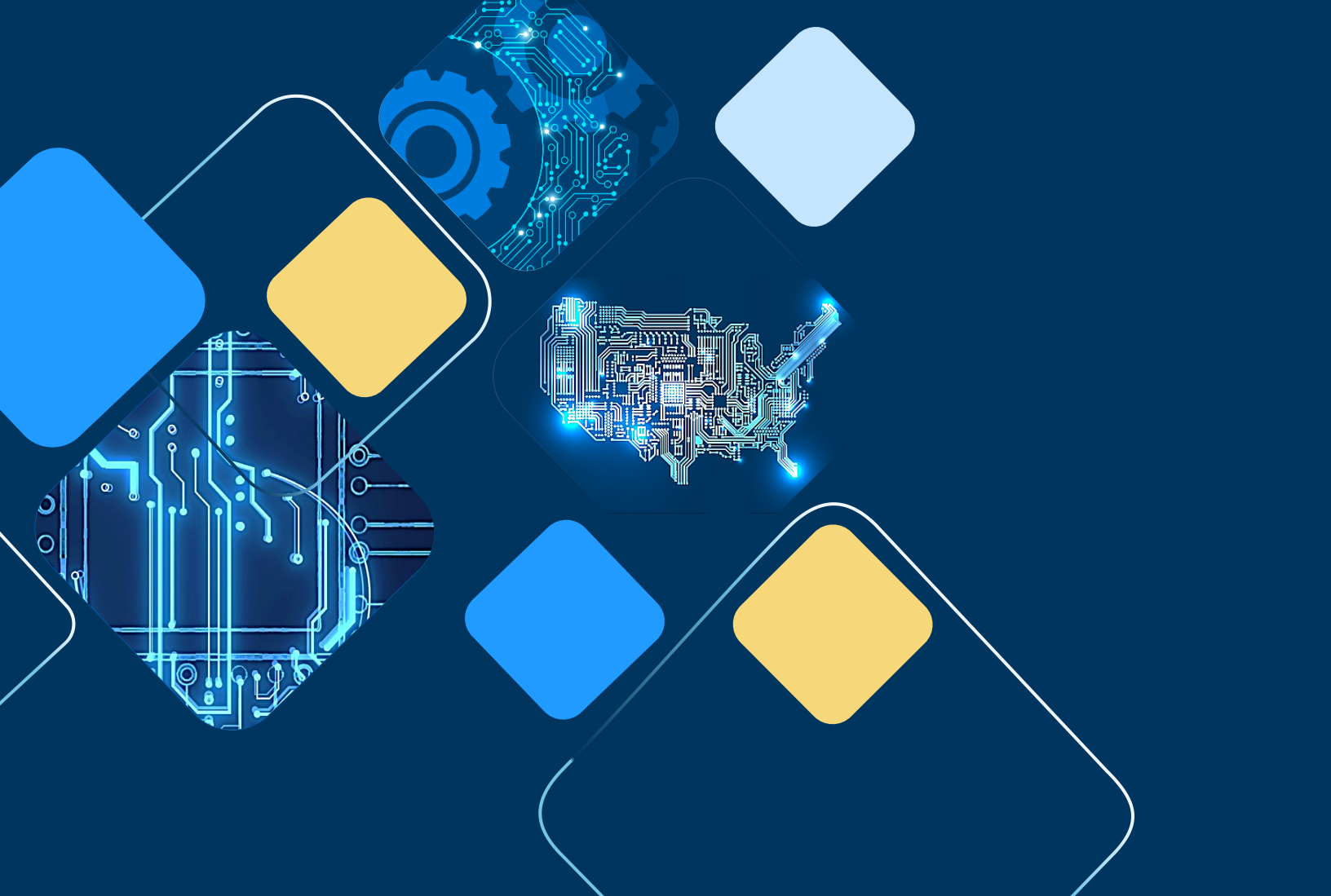




Top Management and Performance Challenges Facing the Department of Commerce in Fiscal Year 2027

October 1, 2026
Report OIG-27-001

U.S. Department of
Commerce Office of
Inspector General





October 1, 2026

MEMORANDUM FOR: Secretary of Commerce Howard Lutnick

FROM: Duane E. Townsend
Performing the Duties of Inspector General

SUBJECT: *Top Management and Performance Challenges Facing the
Department of Commerce in Fiscal Year 2027*
Report No. OIG-27-001

Attached is our final report on the Department's top management and performance challenges for fiscal year (FY) 2027.

We are required by statute to annually report the most serious management and performance challenges facing the Department and identify progress made to address them.¹ This report will be included in the Department's *Agency Financial Report* for FY 2026 and posted on [our website](#).

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

Attachment

cc: Paul M. Dabbar, Deputy Secretary of Commerce
Yvette DePinto, Chief of Staff
Brian Epley, Chief Information Officer
Jennifer Hesch, Acting Deputy Assistant Secretary for Administration,
performing the non-exclusive functions and duties of the Chief Financial Officer
and Assistant Secretary for Administration
Operating Unit Heads
Operating Unit Audit Liaisons

¹ 31 U.S.C. § 3516(d).



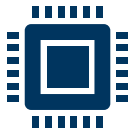


About This Report

The Department of Commerce plays a central role in implementing efforts to advance the nation's economic and technological leadership. As the Department's Office of Inspector General, our mission is to improve the Department's programs and operations through independent and objective audits, investigations, and evaluations. We follow established governmental standards to accomplish our work and report our results to departmental leadership and Congress.

We are required by statute to annually report the most serious management and performance challenges facing the Department and to identify progress made to address them.¹ On the following pages, we summarize the Department's most serious challenges for fiscal year (FY) 2027. We base our assessments on our work as well as trusted scientific and governmental resources.

The summaries are grouped into the following three challenge areas:



Safeguarding National Security and American Business Interests

Protecting national security while promoting American business dominance in advanced technology.



Providing Effective Stewardship of Taxpayer Dollars

Funding and managing programs and operations while protecting taxpayer dollars from fraud, waste, and abuse.



Delivering High-Quality, Reliable Services

Providing essential data and services related to population counts, public safety, weather, and more.

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

Our recent work related to these challenges is listed in the appendix. Visit [our website](#) for more information and to view our other reports. To report fraud, waste, and abuse in the Department's bureaus and programs, contact [our hotline](#).



Contents

Safeguarding National Security and American Business Interests.....	1
Chip Export Authorization Spotlights Challenges for BIS.....	1
Recent Progress on Challenges Must Be Sustained	2
Providing Effective Stewardship of Taxpayer Dollars.....	4
Broadband Grant Programs May Offer More Flexibility, but Fraud Risk Remains a Major Concern	4
Funding Management and Oversight Must Be Improved Across All Programs	6
Delivering High-Quality, Reliable Services	8
Planning and Preparation Increase in Importance as 2030 Census Approaches	8
Challenges Continue for Nationwide Public Safety Broadband Network	9
Cybersecurity Remains a Critical Concern as SI Risks Increase.....	10
NOAA Must Address Challenges in NWS Transformation to Improve Mission Delivery	11
Integrity and Trustworthiness Are Essential to the Department’s Ability to Meet Its Mission	11
Appendix. Relevant OIG Reports and Ongoing Projects.....	13
References	17

Graphics from Adobe Stock except where otherwise credited.



Safeguarding National Security and American Business Interests

The Department's primary management challenge for FY 2027 is to safeguard national security and American business interests. To do this, the Department must enhance its capabilities to prevent the diversion of sensitive products subject to export controls, such as semiconductor technologies, to foreign adversaries.

Countries such as China, Russia, and Iran actively attempt to improve their military capabilities by obtaining U.S. goods and technologies.² The Department's Bureau of Industry and Security (BIS) administers and enforces U.S. export control laws and regulations, thus working to protect sensitive goods and technologies.

The administration's goals of bolstering the domestic manufacturing of semiconductors and prioritizing trade enforcement mean the Department must strike a balance: supporting the objective of establishing the United States as a worldwide leader in artificial intelligence (AI; now referred to as *super intelligence*, or SI³) technologies while at the same time preventing the diversion of that technology to our adversaries. For this balance to be achieved, BIS must address longstanding staffing, oversight, and IT challenges in order to better track and monitor controlled, sensitive items over time and across borders.

Chip Export Authorization Spotlights Challenges for BIS

In July 2025, the President signed Executive Order 14320, *Promoting the Export of The American AI Technology Stack*,⁴ which established the American AI Exports Program. These exports include cutting-edge U.S. technology, and the strongest enforcement will be necessary to keep this technology from being diverted into the hands of adversaries such as China.

The Department announced in a statement⁵ that export approvals for this technology are conditioned on companies meeting "rigorous security and reporting requirements" and that BIS will monitor compliance on an ongoing basis. If BIS does not continuously strengthen its oversight, enforcement, and outreach mechanisms—including increasing resources for export enforcement agents, expanding global monitoring through export control officers, and refining risk assessment criteria—there is a risk that adversaries may circumvent export controls, leading to unauthorized transfers of sensitive American SI technologies.

Our previous work has shown that BIS has limited capacity for this type of monitoring. Specifically, BIS's staff of export control officers, who analyze and monitor millions of high-risk exports per year

for compliance with export regulations, comprised 17 officers worldwide as of September 2026, according to a BIS official—and areas such as Africa and South America had no resident officers at all.⁶ BIS anticipates this number to increase to 25 by the end of calendar year 2026, more than doubling the number of officers previously on staff.

These officers conduct end-use checks, which verify that high-risk items are used only for intended purposes and by intended parties. However, they do so on only a portion of exported items per year.⁷ As highlighted in our May 2026 audit of BIS’s enforcement of Russia and Belarus export controls, BIS issues an annual

targeting strategy for specialists to use when selecting end-use checks on licensed and unlicensed EAR-controlled export transactions. Priority is given to exports involving dual-use items (items with commercial [civilian] and military applications), high-risk items, or emerging technologies, or those destined for regions of strategic concern such as Russia and Belarus.⁸ However, this audit also revealed that

BIS did not adequately document its processes or establish detailed procedures for end-use checks, nor did it require export control specialists to apply consistent methodologies or conduct risk assessments when selecting exported items for end-use verification.⁹ This increases the risk that BIS is not verifying the highest-risk items for these critical checks.

In addition, BIS’s export enforcement information systems are outdated and fall far short of meeting its needs.¹⁰ This is especially critical given the current strategic competition, in which foreign adversaries—particularly those employing advanced evasion tactics and accelerating technological development—are rapidly increasing the sophistication and scale of their efforts to circumvent U.S. export controls.

Recent Progress on Challenges Must Be Sustained

Now that American SI tech stack exports are being approved, BIS must monitor and enforce the “rigorous security and reporting requirements” put in place as a condition of the approvals.¹¹ In essence, the approval of these chip exports has expanded BIS’s role from being a regulatory and domestic enforcer to an ongoing supervisor and global risk manager. To ensure success, BIS must carefully execute its oversight strategy and address its challenges.

After receiving an additional \$44 million in its FY 2026 appropriation,¹² BIS began hiring export specialists and export control officers. The bureau also intends to increase the number of export control officers in FY 2027, which will allow them to expand coverage to other countries. And, in testimony to Congress about a potential FY 2027 funding increase, the Secretary of Commerce commented that an increase would allow the bureau to protect American innovation by adding hundreds of new special agents to its staff.¹³

BIS conducts end-use checks on just a portion of exported items each year:

✦ **1,151** in 2022

✦ **1,509** in 2023

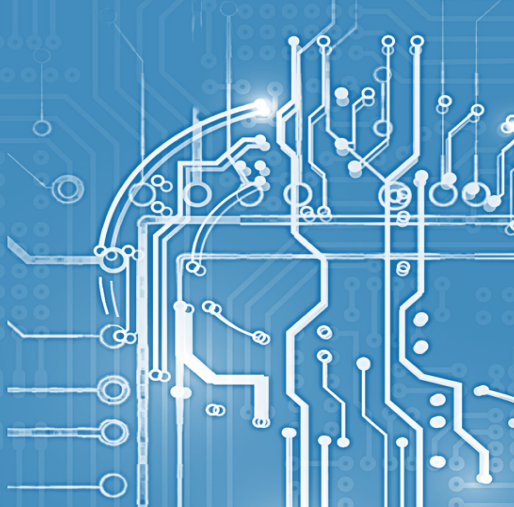


Although BIS has made progress in hiring and training employees, these new employees must gain real-world expertise to be effective in these highly specialized positions. Successfully integrating a newly expanded workforce will be essential for BIS as it seeks to protect sensitive exports worldwide.

In addition, BIS should continue to accelerate and sustain efforts to modernize its IT systems to ensure that it can outpace the increasingly sophisticated methods bad actors use to evade U.S. export controls.¹⁴ Modern, data-driven capabilities are essential for identifying illicit networks, closing enforcement gaps, and safeguarding national security in a rapidly evolving threat environment. The size and complexity of this modernization effort add to the challenge; for any funding BIS receives, it will need to plan and oversee this effort with the utmost care if it is to avoid waste and inefficiency and achieve the greatest benefit possible.

Beyond addressing its staffing and technical needs, BIS needs to strengthen its end-use check process to better identify and prevent restricted shipments. Deficiencies in BIS's export operations could lead to the diversion of, reexport of, or unauthorized access to advanced technologies, and violators might not be held accountable. The Department also faces reputational risk if oversight, monitoring, and reporting are not sufficiently robust and effective.

The Department must continue to strengthen BIS's long-term capacity—by investing in sustained staffing, developing robust information systems and monitoring frameworks, and improving the effectiveness of its oversight—if it is to meet this critical challenge in FY 2027 and beyond.



Providing Effective Stewardship of Taxpayer Dollars

The Department's mission is to "create the conditions for economic growth and opportunity for all communities." To carry out this mission, the Department funds programs and operations through grants, contracts, cooperative agreements, and direct funding. A major challenge for the Department in FY 2027, as with previous years, is spending those funds wisely and providing strong oversight to funding recipients.

The Department awards grants for a wide variety of purposes, including expanding broadband coverage and helping communities rebuild after disasters. It also spends billions in contracts to fund programs and activities that aim to optimize its operations and serve the American people. Between October 2023 and August 2026, the Department's contract and grant obligations totaled approximately \$64.2 billion.¹⁵

With so much funding passing through the Department, strong safeguards are critical to prevent fraud and waste before they happen and to recover fraudulent or improper payments after they occur. Our audits, evaluations, and investigations have repeatedly revealed significant deficiencies in the Department's grant and contract planning and oversight—deficiencies that can contribute to greater fraud risk, potential ballooning costs, and misuse of taxpayer funds. While such challenges are not unique to the Department, its extensive funding portfolio and the importance of its programs to national, state, and local economies make improvement challenging—but essential.

\$64.2 Billion

Approximate total of
Department grants and contracts
Oct. 2023–Aug. 2026

Broadband Grant Programs May Offer More Flexibility, but Fraud Risk Remains a Major Concern

One example of this challenge is in the National Telecommunications and Information Administration (NTIA), which administers and oversees six grant programs with a total appropriation amount of nearly \$49.8 billion. These programs share the ambitious goal of expanding the nation's broadband internet access and adoption.¹⁶

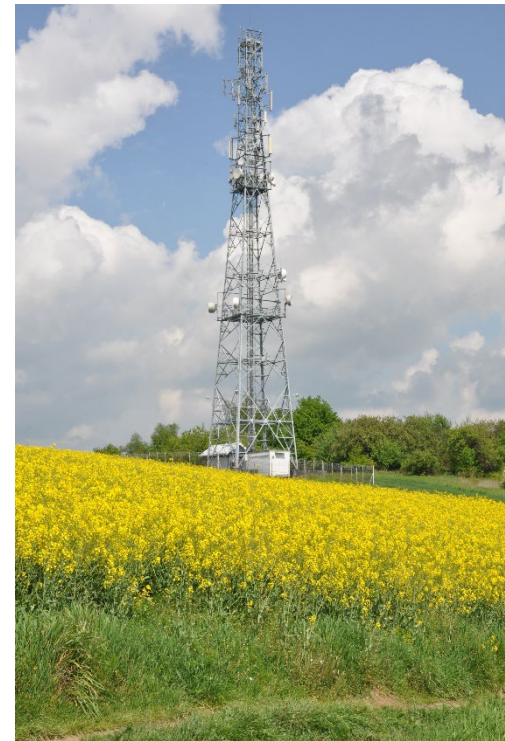
As we explained in last year's *Top Management Challenges* report, some of the programs' technology requirements and regulations have been relaxed.¹⁷ Significantly, in the summer of 2025, NTIA restructured the Broadband Equity, Access, and Deployment (BEAD) Program, which is the largest of the programs at nearly \$42.5 billion.¹⁸ Changes included the removal of several nonstatutory requirements from the original notice of funding opportunity, such as requirements related to labor, employment, and workforce development; adoption of technology neutrality (rather than the original prioritization of fiber-optic projects); and the implementation of new selection processes for subgrantees. These changes have expanded broadband project options for states. However, the changes have also delayed BEAD implementation,¹⁹ requiring grantees to revisit their project plans and possibly delaying projects and expenditures.

Beyond these concerns, our Office of Investigations (OI) has identified a wide variety of fraud schemes related to broadband programs, particularly the \$3 billion Tribal Broadband Connectivity Program. These schemes occur at both the grantee and subgrantee levels, and subgrantee monitoring continues to be a challenge for all broadband programs. The award disbursement rate in programs like these tends to climb as grants enter or continue the construction phase, meaning programs would need to increase their monitoring and oversight to prevent and detect fraud in disbursed funds.

One potential indicator of fraud in these grants is applicants inflating the estimated amount needed to build or expand broadband service—specifically, by applying for grants for locations that are not actually eligible for service, either because those areas already have broadband or funding for service was already received from other sources. Verifying that locations proposed for service are truly unserved or underserved by broadband helps to ensure that grant funding will benefit the locations and communities that need it.

The Department has begun taking steps to raise awareness of fraud risks. The Office of Acquisition Management is proposing a new award condition for fraud prevention, which will require key personnel from grantees, co-grantees, and subgrantees to complete fraud awareness training and report to the Department that they have done so. If the Department adopts this condition, the training will aim to reinforce recipients' fraud prevention and reporting requirements. Additional fraud prevention and awareness measures for subgrantees will seek to mitigate fraud and misappropriation of funds at all levels.

OI continues to expand its outreach to NTIA grant and program personnel, providing fraud awareness briefings that cover current fraud trends and indicators and sharing oversight concerns with stakeholders across all NTIA grant programs. In addition, OI will continue to analyze available information and coordinate with other federal programs to ensure the accuracy of locations identified as unserved or underserved.



Funding Management and Oversight Must Be Improved Across All Programs

The Department has a responsibility to spend taxpayer dollars wisely, including robust oversight of funding recipients and careful management of funding programs. However, our audits, evaluations, and investigations have repeatedly revealed management and oversight deficiencies in the Department's programs. When present, such weaknesses can undermine the Department's ability to prevent, detect, or respond to misuse of funds. Below we provide examples of several contract and grant programs that illustrate these challenges.

As a first example, NOAA is acquiring its next generations of satellites, ships, and aircraft, which collect environmental data for weather forecasting, fisheries management, and coastal mapping. These expensive multiyear efforts must be well-managed to ensure that capabilities meet NOAA's needs and are delivered on schedule and within budget:

- In 2025 and 2026, the Department and NOAA replanned NOAA's GeoXO satellite program, focusing on a weather-only data mission and reducing lifecycle costs by approximately \$7 billion. To achieve the intended savings, some contracts will be renegotiated and others terminated, and controls must be adequate to monitor contractor performance and manage risk. Our March 2026 GeoXO evaluation found that the program's risk management processes need improvement to ensure success.²⁰
- The design and construction of four new "hurricane hunter" aircraft, two oceanographic research ships, and two hydrographic charting and survey ships, as well as the modernization of five fishery survey vessels, is underway. The total projected cost for this work is over \$2.1 billion. NOAA must maintain rigorous contract management and quality assurance to ensure that these assets are mission-ready when they join the fleet.²¹

Our work over the past 15 years has also revealed longstanding problems with the National Institute of Standards and Technology's (NIST's) Hollings Manufacturing Extension Partnership (MEP) program, in which NIST enters into cooperative agreements with various organizations with the goal of enhancing the productivity and technological performance of U.S. manufacturing. For instance:

- A 2026 audit found that the Ohio Department of Development, which operates the Ohio MEP Center, did not comply with MEP award terms and conditions, particularly the requirement to ensure allowable spending and accurate reporting of program income. We questioned \$20.9 million in costs and identified nearly \$2.8 million in underreported program income.²²
- In 2024, we found that MEP's data about its impacts on the U.S. economy are inaccurate and unreliable. As a result, NIST removed MEP's annual economic impact reports for FYs 2020 through 2024, raising questions about the program's performance despite its annual \$175 million price tag.²³

Overall, our work shows that NIST must improve its program management, including taking action to hold award recipients accountable for complying with key award terms, and ensure that taxpayer money is spent appropriately.

In another example, Congress has appropriated nearly \$2 billion to the Economic Development Administration (EDA) to support economic recovery in areas affected by natural disasters between 2021 and 2024.²⁴ Historically, management of such grant programs has been challenging for EDA; grants are often distributed as quickly as possible after disasters, and adequate planning and oversight may not be in place as funds begin going out.²⁵ This can create a rich environment for fraud, waste, and abuse.

Finally, we have reported several times on issues involving the Department's 2020 contract to replace several highly customized financial systems with a single, modern system of commercial off-the-shelf applications, the Business Applications Solution (BAS). One year after the \$341 million contract was awarded, we alerted the Department that it needed to develop key inputs and align with known best practices.²⁶ Two subsequent audit reports pointed to a failure to implement basic management controls;²⁷ the more recent report also found that changes in BAS to fix issues experienced by NOAA

will likely result in significant cost increases. Congress has also expressed concerns about failures, delays, and cost overruns. To address this, we have initiated an audit to assess the effectiveness of the Department's past performance evaluations and oversight of awards to the BAS contractor.²⁸

In these and other programs, strengthening oversight through core internal controls will be critical for the Department to ensure better stewardship of federal funds. Without strong oversight, the Department risks approving, disbursing, and managing grants, contracts, and other agreements without reliable evidence that the funds entrusted to it will be used as intended.

Congress has expressed concerns about **delays, failures, and cost overruns** associated with the BAS system.

Delivering High-Quality, Reliable Services

The Department's third top management challenge area is a continuation of our previous years' *Top Management Challenges* reports: delivering accurate data and top-quality services to its stakeholders.

While the Department's 13 bureaus and offices all have different purposes and missions, they share the obligation to provide first-rate data and services to the public and other stakeholders, including Congress, industry, other nations, and more. Taxpayers must get their money's worth, and stakeholders must be able to trust and rely on the data and services the Department provides.

As with the other challenges summarized in this report, our work has shown that planning and oversight deficiencies have impeded the Department's success and added risk to its operations. This year, the 2030 census, though still in the planning stages, is already a complex and challenging operation that leaves little room for error. In addition, the continued inadequate oversight of the broadband network dedicated to public safety still poses a challenge, as does the Department's need for more effective cybersecurity—especially as SI risks continue to increase along with SI's technological capabilities—and NOAA's ongoing transformation of the National Weather Service (NWS). To address these issues, the Department must commit to taking strong action to increase the integrity and effectiveness of its services.

Planning and Preparation Increase in Importance as 2030 Census Approaches

The 10-year census of the nation's residents provides the data needed to apportion the U.S. House of Representatives and to distribute some \$2.8 trillion in federal funding²⁹ to states, tribal governments, and local communities for services and infrastructure. The profound effect this data has on the life of every person residing in the United States calls for the highest level of accuracy.



The upcoming 2030 census is a massive program—planning began in 2019, and the program will not end until 3 years after the count.³⁰ In FY 2027, the Census Bureau must make sure its plans for 2030 will provide enough oversight over the count and follow-up operations to ensure the

accuracy of its data—data that will help stakeholders make important political, economic, and social policy decisions that affect the entire nation.

As the bureau plans to ramp up hiring and conduct testing in preparation for the 2030 census, it needs to ensure that it has a sufficient budget to evaluate initiatives untested during its 2026 Census Test, one of two major tests to measure the effectiveness of census systems and methods. Without adequate testing, the bureau will not be able to verify that its census operations will work as intended.

The bureau's two major planned tests are the 2026 Census Test, which began on May 1, 2026, and the Dress Rehearsal, which will take place in 2028 (the bureau will refine its operational plan as needed after the tests end). The 2026 test's goals were to test two key priorities: (1) piloting in-field enumeration by the U.S. Postal Service, and (2) enhancements and innovations to field infrastructure, staffing, and training.³¹ The test results will have an impact on both the 2028 rehearsal and the 2030 census and could reveal challenges that may affect the bureau's ability to collect reliable data. The bureau will have to act quickly to address any such challenges in time to ensure the accuracy and value of the data it collects in 2030.

Challenges Continue for Nationwide Public Safety Broadband Network

The Nationwide Public Safety Broadband Network (commonly known as FirstNet) was developed to give first responders across the nation a dedicated, reliable wireless network for emergency response communication. FirstNet Authority, an independent authority within NTIA, manages and oversees the network and is responsible for managing and administering a \$6.5 billion, 25-year contract to deploy and operate it. Public safety users rely on FirstNet to communicate with other emergency responders, dispatchers, and the public during emergencies.

As we have reported multiple times over the past decade, FirstNet Authority has not effectively managed and overseen the contract, including holding the contractor responsible for meeting its requirements.³² Most recently, in April 2026, we reported on FirstNet Authority's overreliance on the contractor to confirm that the network is available and that only eligible users in public safety roles can access it.³³

A network dedicated to first responders must maintain reliability. If the service is not consistently available during emergencies, when first responders need it most, critical public safety communications may be delayed—or may not be able to happen at all. Our work has found that oversight deficiencies may contribute to issues with network performance and even security:

- In December 2024, we reported that FirstNet Authority's lack of oversight was a factor in network performance problems that occurred in the wake of the August 2023 Maui wildfires.³⁴
- In July 2024, we alerted FirstNet Authority management that a 3-hour network outage in February of that year, coupled with a lack of communication and transparency by the contractor and FirstNet Authority about the network's performance, put public safety at jeopardy and posed a risk to the readiness of first responders across the country.³⁵

- Most recently, in August 2026, we cautioned NTIA and FirstNet Authority leadership that independent cybersecurity oversight is needed to protect the network, which is a high-value target for cyberattacks; despite this need, the network’s current governance structure presents its own risk by restricting opportunities for government entities to conduct independent cybersecurity testing and oversight.³⁶

The 2012 law that created the network included a February 2027 statutory sunset for FirstNet Authority.³⁷ As of August 2026, a reauthorization of its authority is pending in Congress. Whatever changes may result from the reauthorization, the Department must address these serious challenges.

Cybersecurity Remains a Critical Concern as SI Risks Increase

The Department and its bureaus deliver services that are essential to the country. Weather prediction, patent processing, census administration, and economic analysis touch the lives of every American. To fulfill its various missions, the Department relies on hundreds of computer systems and a high volume of data that must be safe, secure, reliable, and available.

Unfortunately, cybersecurity risks continue to evolve, increasing the challenges the Department must face. As SI tools are incorporated into hackers’ toolboxes, the speed and scope of potential attacks is increasing. In June 2026, intelligence agencies from five countries, including the United States, announced that SI is not a future consideration—it is already here, and it “accelerates the speed, scale, and sophistication of cyber threats.”³⁸ Their alert was a call to action for cybersecurity leaders and practitioners. Less than a month later, OpenAI, a leading SI company, announced that two of its models had unexpectedly escaped a contained testing environment and hacked another organization.³⁹ This act signaled a significant shift in threat level and made it clear that SI and security are intertwined.

Securing its systems has long been a challenge for the Department. Our *Top Management Challenges* reports and oversight work have highlighted ongoing weaknesses with the effectiveness of the Department’s cybersecurity program, particularly with respect to consistent implementation of security controls. Those weaknesses lead to security vulnerabilities that could be leveraged by our SI-enabled adversaries. While the Department has incorporated new protection technologies, our reports continue to highlight areas where security control implementation and monitoring require further improvement.

The Department and its bureaus use IT systems to . . .

- ✱ Monitor exports
- ✱ Process grants and contracts
- ✱ Track economic trends
- ✱ Analyze demographic data
- ✱ Generate weather forecasts
- ✱ Process patents and trademarks
- ✱ Develop scientific and technical standards
- ✱ Maintain cybersecurity databases

. . . and much more.

A key service NIST provides to the cybersecurity community will also likely be strained. In a May 2026 evaluation, we found that NIST has experienced challenges in keeping up with increasing volumes of submissions to its public-facing National Vulnerability Database, which catalogs security flaws and weaknesses in IT infrastructure that could be exploited by bad actors. In our report, NIST cites a 263 percent increase in submissions between 2020 and 2025, leading to an overwhelming number of new vulnerabilities that NIST must analyze and publish in the database.⁴⁰ This will likely accelerate as new SI capabilities become available to the public.

The Department is uniquely positioned to act on SI governance and cybersecurity at a national level. As we discussed in the first challenge in this report, BIS is tasked with ensuring that exports of powerful technologies are managed—and, to a certain extent, preventing other countries from matching America’s lead. And NIST, through its standard-setting and research capabilities, will guide the use, security, and testing of SI to enhance cybersecurity preparation and defense. The Department’s ongoing challenge will be to keep pace with rapid SI developments and ensure up-to-date cybersecurity, both in the broader security ecosystem and in its internal capabilities.

NOAA Must Address Challenges in NWS Transformation to Improve Mission Delivery

NOAA’s ongoing transformation of NWS intends to modernize NWS’s delivery of services. It involves both system and staff adjustments: moving critical systems to cloud computing environments and realigning NWS staff to accommodate future needs. Challenges in both areas must be met if NWS is to continue to protect the public from weather and water disasters.

While cloud computing offers many advantages, NWS must manage its transitions in an environment where the demand for cloud computing resources has increased significantly. Moreover, NWS’s goal is to operate its entire production suite of forecast models in the cloud by December 2027—an aggressive timeline that will require strong management to ensure technical readiness. And changes to the government’s cloud computing oversight program will likely significantly increase the burden on staff to maintain sufficient data security in a cloud environment.⁴¹

In addition, in 2026 NWS planned to complete a staff reorganization with the goal of modernizing operations while ensuring the timely delivery of high-quality meteorological products. NWS was also hiring over 200 new entry-level meteorologists. This infusion of new talent will require a closely managed training and development program to fully realize their potential in the new organizational structure.

Integrity and Trustworthiness Are Essential to the Department’s Ability to Meet Its Mission

Census data, FirstNet operations, the National Vulnerability Database, and weather forecasting are just a few of the many services the Department provides. The public and other stakeholders need to be able to trust that the Department’s services are reliable and delivered with integrity.

When that trust is broken—whether through inadequate oversight or through fraud or other misconduct—restoring it can be difficult.

Our investigations regularly uncover individual examples of wrongdoing, including wire fraud and embezzlement, ethics issues, misuse of position, and retaliation.⁴² In 2025, for example, we substantiated allegations that officials at a bureau had interfered with our audits by altering or withholding documents, intimidating employees, and improperly monitoring employees' communications with auditors. In a related investigation, we substantiated allegations that a bureau official had retaliated against an employee for providing us with information in support of our audits.

Even though misconduct undermines the public's trust, corrective action can make a difference. After we began receiving hotline referrals from United States Patent and Trademark Office (USPTO) management about potential conflicts of interest involving USPTO patent examiners, we opened multiple investigations as well as an evaluation. The evaluation, issued in 2024, uncovered a long-standing deficiency in ethics oversight among patent examiners,⁴³ and OI continued investigating the most serious allegations. OI has also worked with USPTO to resolve conflict-of-interest allegations against two patent examiners, resulting in settlement agreements in February and March 2026 totaling more than \$620,000 to the government.⁴⁴ Our work also helped prompt USPTO to issue new guidance on patent examination and stock ownership in March 2026.⁴⁵

When ethical concerns arise at the Department, it needs to commit to identification and prevention as it responds to the issues and collaborates with our office. And, as the Department works toward meeting its challenges in FY 2027, we will continue providing objective, effective oversight of its programs and operations.



Appendix.

Relevant OIG Reports and Ongoing Projects

National Security and American Business Interests

Completed Work Since FY 2024

- *Audit of BIS's Enforcement Efforts to Combat China's Military-Civilian Fusion Strategy* ([OIG-26-021-A](#))
- *Audit of BIS's Enforcement of Russia and Belarus Export Controls* ([OIG-26-019-A](#))
- *BIS Needs to Improve Its Incident Response Capabilities to Handle Sophisticated Cyberattacks* ([OIG-25-022-I](#))
- *BIS's 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](#))
- *ITA Did Not Effectively Resolve Foreign Trade Barriers* ([OIG-24-004-A](#))
- *Management Alert: Excluding Deemed Exports and Reexports from 15 C.F.R. § 742.6(a)(6) Could Pose a Significant Risk of Unauthorized Technology Release to China's Military* ([OIG-24-001-M](#))

Ongoing Oversight Projects

- *Audit of the International Trade Administration's Antidumping and Countervailing Duty Verification Process* ([2025-526](#))
- *Audit of BIS's Strategy for Identifying and Selecting for Review Exports at Risk of Diversion to China* ([2024-494b](#))

Stewardship of Tax Dollars

Completed Work Since FY 2024

- *Audit of NIST's Assessment of Applicant Eligibility for CHIPS Incentives Funding* ([OIG-26-030-A](#))
- *Audit of NTIA's Public Wireless Supply Chain Award Process for NOFO 1 [Notice of Funding Opportunity 1]* ([OIG-26-027-A](#))
- *Audit of NIST MEP Awards to Ohio Department of Development* ([OIG-26-025-A](#))
- *Audit of Administrative Funds for NTIA Broadband Programs* ([OIG-26-022-A](#))
- *Audit of NTIA's Review of the Broadband Equity, Access, and Deployment Program's Planning Phase Requirements* ([OIG-26-018-A](#))
- *Evaluation of the Management and Oversight of the Class B Ship Acquisition Program by NOAA's Office of Marine and Aviation Operations* ([OIG-26-014-I](#))

- *NTIA Broadband Programs: Semiannual Status Report* ([OIG-26-013-I](#))
- *Audit of MBDA Business Center Program* ([OIG-26-001-A](#))
- *NTIA Broadband Programs: Semiannual Status Report* ([OIG-25-031-I](#))
- *EDA Needs to Improve Oversight of CARES Act Revolving Loan Funds to Ensure Loans Are Made to Eligible Borrowers and Used as Intended* ([OIG-25-019-A](#))
- *NTIA Established the Innovation Fund Program but Needs a Plan to Ensure That the Program Meets Statutory Objectives* ([OIG-25-017-I](#))
- *Broadband Stakeholders Identified Various Challenges Affecting Broadband Deployment* ([OIG-25-014-I](#))
- *OIG's Evaluation of MEP's Economic Impact Reporting Process Also Identified Instances of Noncompliance at Centers, Led to NIST Action* ([OIG-25-011-I](#))
- *Semiannual Status Report on NTIA's Broadband Programs* ([OIG-24-033-I](#))
- *NTIA's Award Processes Leave Tribal Broadband Grants Vulnerable to Fraud and Duplication* ([OIG-24-019-A](#))
- *Management Alert: Challenges Industry Stakeholders Face with Broadband Deployment* ([OIG-24-015-M](#))
- *The Department Needs to Improve Oversight to Ensure the Success of Its Financial System Modernization* ([OIG-24-014-A](#))
- *Semiannual Status Report on NTIA's Broadband Programs* ([OIG-24-012-I](#))
- *EDA Generally Monitored Grants Awarded Under the FY 2019 EDA Disaster Supplemental Notice of Funding Opportunity* ([OIG-24-005-A](#))

Ongoing Oversight Projects

- *Audit of NIST's National Semiconductor Technology Center* ([2026-547](#))
- *Audit of NIST's Oversight of Semiconductor Incentives Program Disbursements* ([2026-546](#))
- *Audit of EDA's Pre-Award Processes for FY 2023 Disaster Relief Funds* ([2026-545](#))
- *Semiannual Evaluation of the Status of NTIA's Broadband Grant Programs* ([2026-544](#))
- *Audit of NTIA's Oversight of Public Wireless Supply Chain Innovation Fund NOFO 1 Grant Funds* ([2026-543](#))
- *Evaluation of NOAA's Class B Ship Design and Construction* ([2026-537](#))
- *Evaluation of Cybersecurity and IT Contract Performance* ([2026-533](#))
- *Audit of NTIA's Oversight of Digital Equity Program Expenditures* ([2026-529](#))
- *Audit of Middle Mile Broadband Infrastructure Program Funds Awarded by NTIA* ([2026-527](#))
- *Audit of NTIA Grants Awarded to Connecting Minority Communities Pilot Program Recipients* ([2025-519](#))
- *Audit of the Department's Performance Evaluations and Oversight of the BAS Contractor* ([2025-516](#))
- *Audit of NIST's Semiconductor Incentives Program Eligibility* ([2025-512](#))
- *Audit of BAS system implementation for the Census Bureau* ([2025-510](#))
- *Audit of EDA's FY 2019 Disaster Relief Grant Costs Claimed and Oversight* ([2025-509](#))
- *Audit of NTIA's Allocation of BEAD Funds* ([2024-498](#))

High-Quality Services

Completed Work Since FY 2024

- *Management Alert: Oversight Issues Observed During the 2026 Census Test* ([OIG-26-031-I](#))
- *Management Alert: Technological Issues Observed During the 2026 Census Test* ([OIG-26-029-I](#))
- *Management Alert: Operational Issues Observed During the 2026 Census Test* ([OIG-26-028-I](#))
- *Management Alert: Oversight Challenges Due to Shared NPSBN Network Architecture* ([OIG-26-026-I](#))
- *Evaluation of NIST's Management of the National Vulnerability Database* ([OIG-26-020-I](#))
- *NWS Actions Relevant to the Catastrophic Flash Flood in Texas* ([OIG-26-017-I](#))
- *Audit of the First Responder Network Authority's Oversight of User Eligibility for the Nationwide Public Safety Broadband Network* ([OIG-26-016-A](#))
- *Audit of the First Responder Network Authority's Oversight of Service Availability for the Nationwide Public Safety Broadband Network* ([OIG-26-015-A](#))
- *Evaluation of the Methodology the Census Bureau Used to Select the Test Sites for the 2026 Census Test* ([OIG-26-012-I](#))
- *Audit of Data Collection and Quality Control Procedures for the U.S. Census Bureau's American Community Survey* ([OIG-26-010-A](#))
- *Evaluation of NOAA's Progress Implementing the GeoXO Satellite Program* ([OIG-26-009-I](#))
- *Evaluation of the Space Weather Follow-On Program's Progress in Preparing the SWFO-L1 Satellite for Launch and Operations* ([OIG-26-008-I](#))
- *Audit of the Department's Vulnerability Reporting and Resolution Program* ([OIG-26-002-A](#))
- *Audit of the Census Bureau's Progress in Meeting Workforce Hiring Goals for the 2026 Census Test* ([OIG-25-030-A](#))
- *Audit of USPTO's Quality Reviews of Continuing Patent Applications* ([OIG-25-029-A](#))
- *Independent Evaluation of the National Oceanic and Atmospheric Administration's National Weather Service Tornado Forecasting and Warning Services* ([OIG-25-026-I](#))
- *USPTO Should Improve Governance to Promote Effective Oversight of Its Artificial Intelligence Tools* ([OIG-25-018-A](#))
- *The Census Bureau Should Address Challenges from the 2020 Post-Enumeration Survey Ahead of the 2030 Census* ([OIG-25-015-A](#))
- *The National Weather Service Should Further Strengthen Its Protection of Essential Operational Technology* ([OIG-25-012-I](#))
- *Data Quality Challenges and Ineffective Program Management Hinder the Department's Enterprise Cybersecurity Capabilities* ([OIG-25-006-A](#))
- *Nationwide Public Safety Broadband Network Was Not Always Available to First Responders During the Catastrophic 2023 Maui Wildfires* ([OIG-25-004-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](#))
- *A 3-Year Exposure of Privacy Act-Protected Data Revealed USPTO Mismanagement in Safeguarding the Sensitive PII of Trademark Filers* ([OIG-24-029-I](#))

- *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](#))
- *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](#))
- *Management Alert: The NPSBN Band 1 Signal Strength Does Not Consistently Provide Adequate Band 14 Service for First Responders* ([OIG-24-022-M](#))
- *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 Department Needs to Strengthen Its Ethics Oversight for USPTO Patent Examiners* ([OIG-24-013-I](#))
- *The Department Needs to Fully Implement Strong Multifactor Authentication for Its High Value Assets to Protect Them from Cyberattacks* ([OIG-24-009-A](#))

Ongoing Oversight Projects

- *Audit of FirstNet Authority's Innovation and Test Lab* ([2026-548](#))
- *Evaluation of the U.S. Census Bureau's 2026 Census Test Operations* ([2026-541](#))
- *Biennial Audit of the Department's Compliance with Aspects of the Geospatial Data Act* ([2026-535](#))
- *Evaluation of NOAA's Oversight of JPSS Contractors in Preparation for JPSS-3 and JPSS-4 Launch* ([2026-534](#))
- *Evaluation of FirstNet [Authority] Cybersecurity Oversight* ([2026-532](#))
- *Audit of the U.S. Census Bureau's Enterprise Cybersecurity Support Contract* ([2026-531](#))
- *Audit of USPTO's Handling of Patent Applications Containing Sensitive Information* ([2025-525](#))
- *Audit of NWS Staffing* ([2025-523](#))
- *Audit of USPTO's Patent Center System* ([2025-521](#))
- *Audit of the Department's Past Performance Evaluations and Oversight of Contractor* ([2025-016](#))



References

¹ 31 U.S.C. § 3516(d).

² Recent national security threat assessments list China, Russia, Iran, and North Korea as major state actors challenging U.S. interests. (Office of the Director of National Intelligence, March 2025, [2025 Annual Threat Assessment of the U.S. Intelligence Community](#), 9–30; and March 2026, [2026 Annual Threat Assessment of the U.S. Intelligence Community](#), 9–13, 15–32.)

³ Executive Office of the President. September 29, 2026. [Inaugurating the Era of Super Intelligence](#). Accessed September 30, 2026.

⁴ Executive Office of the President. July 23, 2025. [Promoting the Export of the American AI Technology Stack](#). 90 Fed. Reg. 35393. Accessed September 30, 2026.

⁵ Department of Commerce. November 19, 2025. Press Release, “[Statement on UAE and Saudi Chip Exports](#).”

⁶ BIS. “[About BIS: Export Control Officer \(ECO\) Program](#).” Accessed September 30, 2026.

⁷ We analyzed data from the Department’s [Annual Performance Plan and Report, FY 2023–2025](#) for our May 4, 2026, *Audit of the Bureau of Industry and Security’s Enforcement of Russia and Belarus Export Controls*, [OIG-26-019-A](#).

⁸ Commerce OIG. [OIG-26-019-A](#), 2–3.

⁹ Commerce OIG. [OIG-26-019-A](#), 7, 11–13.

¹⁰ Commerce OIG, June 23, 2026, *Audit of the Bureau of Industry and Security’s Enforcement Efforts to Combat China’s Military-Civilian Fusion Strategy*, [OIG-26-021-A](#), 7; and [OIG-26-019-A](#), 8–9.

¹¹ Department of Commerce. “[UAE and Saudi Chip Exports](#).”

¹² Congressional Research Service. February 25, 2026. *Overview of FY2026 Appropriations for Commerce, Justice, Science, and Related Agencies (CJS)*, 11.

¹³ Lutnick, Howard. April 22, 2026. [A Review of the President’s Fiscal Year 2027 Budget Request for the Department of Commerce](#). Testimony of the Secretary of Commerce before the Senate Committee on Appropriations, Subcommittee on Commerce, Justice, Science, and Related Agencies.

¹⁴ Commerce OIG. [OIG-26-019-A](#), 8–9.

¹⁵ Our analysis of spending data from USAspending.gov.

¹⁶ Commerce OIG. February 6, 2024. *Semiannual Status Report on NTIA’s Broadband Programs*, [OIG-24-012-I](#), 1.

¹⁷ Commerce OIG. December 1, 2025. *Top Management and Performance Challenges Facing the Department of Commerce in Fiscal Year 2026*, [OIG-26-003](#), 26–28.

¹⁸ NTIA. June 2025. [BEAD Restructuring Policy Notice](#).

¹⁹ NTIA, [BEAD Restructuring Policy Notice](#); also see the [June 30, 2026, testimony](#) of Assistant Secretary of Commerce for Communication and Information Arielle Roth before the House Energy and Commerce Subcommittee on Communications and Technology, 119th Congress (accessed August 27, 2026).

²⁰ Commerce OIG. March 9, 2026. *Evaluation of NOAA’s Progress Implementing the GeoXO Satellite Program*, [OIG-26-009-I](#).

²¹ Commerce OIG, June 17, 2025, *NOAA Must Take Action to Avoid Gaps in Hurricane Hunter Missions and Improve Oversight, Program Management, and Systems Engineering Practices*, [OIG-25-023-A](#); and April 2, 2026, *Evaluation of*

the Management and Oversight of the Class B Ship Acquisition Program by NOAA's Office of Marine and Aviation Operations, [OIG-26-014-I](#).

²² Commerce OIG. August 19, 2026. *Audit of NIST MEP Awards to Ohio Department of Development*, [OIG-26-025-A](#).

²³ Commerce OIG. September 25, 2024. *NIST Overstated MEP's Economic Impacts to Congress and Other Stakeholders*, [OIG-24-037-I](#).

²⁴ See the American Relief Act, 2025, Pub. L. No. 118-158, Div. B, Title II, 138 Stat. 1722, 1734; and the Consolidated Appropriations Act, 2023, Pub. L. No. 117-328, Div. N, Title II, 136 Stat. 4459, 5204. We received \$9 million for oversight as part of these appropriations. The appendix lists our relevant ongoing and completed audits and evaluations. See also EDA's [FY2025 Disaster Supplemental Notice of Funding Opportunity](#).

²⁵ Commerce OIG. May 11, 2020. *Top Oversight Challenges Facing the Department of Commerce to Ensuring That Pandemic Funds Are Timely and Appropriately Spent*, [OIG-20-026-M](#).

²⁶ Commerce OIG. April 19, 2021. *Management Alert: BAS Program's Focus on Technology May Overlook Risks Related to Business Processes*, [OIG-21-023-M](#).

²⁷ Commerce OIG, July 7, 2022, *The BAS Program Needs to Increase Attention to Business Process Reengineering and Improve Program Management Practices*, [OIG-22-025-A](#); and February 22, 2024, *The Department Needs to Improve Oversight to Ensure the Success of Its Financial System Modernization*, [OIG-24-014-A](#).

²⁸ Commerce OIG. March 20, 2025. *Audit of the Department's Past Performance Evaluations and Oversight of [Contractor] Contracts*, [25-516](#).

²⁹ Villa Ross, Ceci. June 2023. [Uses of Decennial Census Programs Data in Federal Funds Distribution: Fiscal Year 2021](#), 12–23.

³⁰ U.S. Census Bureau. February 10, 2025. [2030 Census Planning Timeline](#). Accessed May 29, 2026. We reproduced this timeline in our March 16, 2026, report, *Evaluation of the Methodology the Census Bureau Used to Select the Test Sites for the 2026 Census Test* ([OIG-26-012-I](#)), 1, 13.

³¹ Census Bureau. May 1, 2026. [2026 Census Test](#). Accessed May 29, 2026. See also [OIG-26-012-I](#), 1.

³² We reported on FirstNet oversight issues in our [Top Management Challenge Reports from FYs 2017 through 2026](#). We have also completed [nine audits and evaluations](#) on these issues in the past 3 years alone. In addition, on August 28, 2025, we issued [two public summaries of investigations](#) into misconduct by FirstNet Authority officials.

³³ Commerce OIG, April 9, 2026, *Audit of FirstNet Authority's Oversight of Service Availability for the Nationwide Public Safety Broadband Network*, [OIG-26-015-A](#); and April 16, 2026, *Audit of FirstNet Authority's Oversight of User Eligibility for the Nationwide Public Safety Broadband Network*, [OIG-26-016-A](#).

³⁴ Commerce OIG. December 5, 2024. *Nationwide Public Safety Broadband Network Was Not Always Available to First Responders During the Catastrophic 2023 Maui Wildfires*, [OIG-25-004-A](#).

³⁵ Commerce OIG. July 28, 2024. *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](#).

³⁶ Commerce OIG. August 24, 2026. *Management Alert: Oversight Challenges Due to Shared NPSBN Network Architecture*, [OIG-26-026-I](#).

³⁷ Middle Class Tax Relief and Job Creation Act of 2012 (Pub. L. 112-96), February 22, 2012.

³⁸ Cybersecurity and Infrastructure Security Agency. June 22, 2026. Blog: [“Five Eyes Cyber Security Agencies Statement.”](#) Accessed July 28, 2026.

³⁹ Kahn, Jeremy and Emily Forlini, [“OpenAI says its AI models Escaped Control and Hacked into AI Company Hugging Face.”](#) *Fortune*, July 21, 2026; and Booth, Harry, [“How OpenAI Lost Control of an AI Model—and What Needs to Change.”](#) *Time*, Jul 24, 2026, 11:13 a.m. EDT. Both accessed July 28, 2026.

⁴⁰ Commerce OIG. May 26, 2026. *Evaluation of NIST's Management of the National Vulnerability Database*, [OIG-26-020-I](#), “NIST's Response” (appendix 4), 37.

⁴¹ See <https://www.fedramp.gov/20x/>.

⁴² Commerce OIG. April 27, 2026. *Semiannual Report to Congress, March 2026*, [SAR-2026-03](#), 15–17.

⁴³ Commerce OIG. February 14, 2024. *The Department Needs to Strengthen Its Ethics Oversight for USPTO Patent Examiners*, [OIG-24-013-I](#).

⁴⁴ U.S. Department of Justice press releases: February 25, 2026, *U.S. Patent and Trademark Office Employee Agrees to Pay \$500,000 to Resolve Conflict-of-Interest Allegations*, [26-189](#); and March 11, 2026, *Former U.S. Patent and Trademark Office Employee Agrees to Pay \$122,480 to Resolve Conflict-of-Interest Allegations*, [26-243](#).

⁴⁵ Memorandum from John A. Squires, Under Secretary of Commerce for Intellectual Property and Director of USPTO, to patent office employees. March 2, 2026. [Guidance on Examination of Patent Applications and Stock Ownership](#). See also our evaluation from February 14, 2024, *The Department Needs to Strengthen Its Ethics Oversight for USPTO Patent Examiners*, [OIG-24-013-I](#).

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