Testimony of

Peggy E. Gustafson
Inspector General

U.S. Department of Commerce
Office of Inspector General

before a hearing of the

Energy and Commerce Committee
Oversight and Investigations Subcommittee
U.S. House of Representatives

March 29, 2023

Introduction

Chairman Griffith, Ranking Member Castor, and members of the subcommittee:

Thank you for your invitation to speak before the subcommittee today. I appreciate the opportunity to testify about the Office of Inspector General's strong oversight of Department of Commerce programs and initiatives. I am grateful for your continued interest in and support of our work. I look forward to our dialogue today and to continued conversation about the important work OIG accomplishes.

Today, I will provide an overview of Commerce OIG's independent oversight of several high-profile areas—the CHIPS and Science Act (CHIPS Act), the Infrastructure Investment and Jobs Act (IIJA), cybersecurity, and oversight of pandemic relief funds. I will also share with you lessons learned and best practices for the oversight of new and emerging programs. Commerce OIG has a positive story to tell about focusing efforts and deploying resources to yield meaningful, high-impact results.

Oversight of Semiconductor Production Reshoring Through the CHIPS Act

The first area I would like to discuss with you today is Commerce OIG's oversight of programs and activities associated with the CHIPS Act. The COVID-19 pandemic and its impacts helped crystalize awareness that our nation's security and economy rely heavily on access to semiconductors. Over the last three decades, the United States' production of semiconductors has decreased; by enacting the CHIPS Act, policymakers have affirmed the need for increased domestic production. The Department will play a key role in executing this law, and OIG is committed to performing oversight.

Implementation of the CHIPS Act

The Department has identified four strategic goals for implementation of the Act:

1. Invest in U.S. production of strategically important semiconductor chips, especially leading-edge technologies.
2. Assure a sufficient, sustainable, and secure supply of older and current-generation semiconductors for national security and critical manufacturing industries.
3. Strengthen semiconductor research and development leadership.
4. Grow a diverse semiconductor workforce and build strong communities that participate in the prosperity of the semiconductor industry.

The Act directs the Department to create a program to spur the recreation of a domestic semiconductor industry and entrusts the Secretary with significant discretion on how the program can be established and implemented.

The Act provides the Department with up to $39 billion in direct funding, up to $11 billion for research and development, and up to $75 billion in direct loans and loan guarantees. The funding may be used for:

- construction, expansion, or modernization of facilities and equipment;
- site development and modernization;
- workforce development; and
- reasonable operating costs (as determined by the Department).

The Act also provides OIG with $25 million over 5 years for CHIPS oversight. We are grateful for the funding, and we are hiring staff for two audit teams to conduct CHIPS program oversight, as well as a team of investigators to focus on the detection and resolution of any fraud committed by recipients of CHIPS funding. We expect the audit staff will include at least one subject matter expert in semiconductor materials and technology. These new teams will be a vital part of OIG's independent, continuous oversight of the program, to include determining whether:

- eligible entities use the funding received under the program in accordance with established requirements;
- entities receiving financial assistance carry out their commitments to worker and community investments;
- the required agreement has been carried out to give covered entities sufficient guidance about violations of the agreement;
- Congress receives timely notification about violations of the required agreement and how that determination was reached; and
- the Department has sufficiently reviewed any covered entity engaging in a listed exception.

Potential Challenges

OIG has already identified preliminary challenges for the Department. One challenge is managing its workforce, to include hiring and training staff quickly to meet new demands. The Department must identify qualified candidates, conduct background checks, and onboard new hires in a timely manner. Additionally, hiring while the program is being implemented may impair the proper assessment of current and future skills gaps, the development of training plans, and the effective allocation of resources.

Additionally, the Department must implement adequate internal controls and oversight. The increased funding may also increase the volume and complexity of financial transactions, thus making it more difficult to detect and prevent payment errors, fraud, waste, and abuse. The increase in funding may require additional monitoring and reporting to ensure project recipients comply with statutes, achieve intended outcomes, and use funds efficiently. Finally, the increased funding may introduce new or emerging risks that must be identified and addressed in a timely fashion.

Improving Broadband Internet Access Through IIJA

OIG is also committed to oversight of the Department's broadband infrastructure funding. By enacting IIJA, Congress highlighted the critical importance of affordable, high-speed broadband for individuals, families, and communities to be able to work, learn, and connect remotely. Increasing access to broadband is an ongoing national challenge.

Implementation of IIJA

In 2021, IIJA provided roughly $65 billion with the stated intention of ensuring that every American has access to reliable high-speed internet. IIJA included investment in broadband infrastructure deployment that builds on investments from previous laws, including the American Rescue Plan Act of 2021 (ARPA) and the Consolidated Appropriations Act, 2021 (CAA). The National Telecommunications and Information Administration (NTIA) will use $48 billion of this funding to implement the following programs:

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

Oversight of IIJA Implementation

OIG is building three audit teams and a team of investigators to focus on broadband issues. We have planned a holistic oversight program to monitor the grant process throughout its lifecycle. We have planned our audit and evaluation work to take part in the following phases:

- Implementation: includes application review, award process, and funds disbursement
- Award Oversight: review compliance with award policies and procedures
- Funds Oversight: monitor appropriate use of funds
- Closeout: measure compliance with closeout procedures

In January 2022, we provided our prior Broadband Technology Opportunities Program (BTOP) work to help the Department plan and prepare for the significant increase in IIJA funding. Additionally, in FY 2018, we issued a report on challenges facing EDA when it received a significant increase in funding for disaster recovery. The report highlighted key oversight challenges and best practices—based on prior OIG reports and other agencies' relevant work—and identified actions EDA should take. These lessons learned can also be applied to grant programs, like IIJA and the CHIPS Act and will help the Department avoid historical pitfalls while implementing its responsibilities under these Acts.

Our IIJA oversight plan is based on an evaluation of NTIA's preparedness to administer and manage increased grant awards. We review and analyze the Department's plans for spending IIJA funds and assess the risk for fraud, waste, or abuse. Based on our initial assessment, we initiated an audit of NTIA's process for awarding grants for the Tribal Broadband Connectivity Program, which is currently the most mature of IIJA programs and has already distributed $1.7 billion. As the Department refines its plans to execute the IIJA, we will refine our IIJA oversight plan.

As part of its oversight, OIG will also issue a series of semiannual reports summarizing the status of IIJA programs. These reports will provide program milestone dates, status of funds awarded to date, status of remaining funding, and oversight findings OIG has reported on. The first report was issued this past January.[1] Finally, within OIG, our audit and investigation teams collaborate to identify areas most susceptible to fraud and abuse.

Improving Cybersecurity While Addressing Longstanding IT Challenges

In addition to oversight for the CHIPS Act and IIJA, Commerce OIG continues to provide oversight for ongoing Department challenges. In May 2021, Executive Order 14028 was issued with the stated purpose of combatting ever-increasing cyberthreats.[2] The executive order moved the government toward zero-trust cybersecurity principles. Implementing the new security requirements presents a challenge for the Department, which must continue to mature its IT security program to address longstanding cybersecurity weaknesses while transitioning to a zero-trust architecture.

In our most recent *Top Management and Performance Challenges* report,[3] OIG again includes the maturation of Commerce's IT security program among the challenges for the Department in FY 2023. OIG has identified several key areas that will require prioritization from the Department, including using multifactor authentication (MFA) Department-wide, modernizing

[1] DOC OIG, January 24, 2023. *Semiannual Status Report on NTIA's Broadband Programs,* OIG-23-009. Washington, DC: DOC OIG.
[2] White House, May 12, 2021. *Executive Order on Improving the Nation's Cybersecurity.* Washington, DC: White House. Available online at https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (accessed July 19, 2022).
[3] DOC OIG, October 13, 2022. *Top Management and Performance Challenges Facing the Department of Commerce in Fiscal Year 2023*, OIG-23-001. Washington, DC: DOC OIG.

legacy systems, and securely managing user accounts and permissions. OIG's recent audit work has highlighted barriers and challenges in these areas.[4,5]

Transitioning to zero-trust architecture also poses a challenge to the Department. Zero trust moves away from a perimeter-defense mindset, allowing for additional protection checkpoints each time a user wants to access data, instead of giving full trust to inside users. Implementing zero trust will require comprehensive changes to the Department's IT security program. Many of the new requirements touch on longstanding challenges that also impact the maturity of the Department's information security program. In fact, the Department has already failed to meet the deadlines for implementing some requirements, such as the requirement to adopt MFA and data encryption Department-wide by November 8, 2021.

OIG has observed improvement in the incident response capabilities of the Enterprise Security Operations Center and the Census Bureau, with the Department taking sufficient action to result in the closure of a number of previously open audit recommendations.[6,7] From FY 2020 to FY 2021, the Department also increased the maturity of two functional areas related to the Federal Information Security Management Act of 2002 (FISMA), and it maintained this improvement in FY 2022.[8] Despite this progress, longstanding weaknesses will remain until the IT security program is consistently implemented across all the Department's bureaus.

Managing and Safeguarding Pandemic-Related Funding

It has been just over 3 years since the COVID-19 pandemic was declared a nationwide emergency. Although restrictions have eased and case numbers have gone down, OIG remains focused on the Department's pandemic-related funding. As with the broadband infrastructure initiative, OIG continues to prioritize the funding the Department received for grants to ease the pandemic's burden on people and businesses.

The total dollar amount of the Department's obligated grant awards increased substantially after Congress passed multiple spending bills allocating funding for pandemic relief. In FYs 2020 and 2021, the Department received more than $6.9 billion under the Coronavirus Aid, Relief, and Economic Security Act (CARES Act), CAA, and ARPA to support the Department's response to the pandemic. For example, the Economic Development Agency's (EDA's) obligated grant award amounts doubled—from $760 million to $1.5 billion— between FY 2019 and FY 2021 and rose again to almost $3.9 billion in FY 2022.

This infusion of funding also increases departmental programs' exposure to potential fraud. One of OIG's top investigative priorities is to pursue fraud associated with the pandemic;

---

[4] DOC OIG, June 15, 2022. *The Department Mismanaged, Neglected, and Wasted Money on the Implementation of IT Security Requirements for Its National Security Systems*, OIG-22-023-I. Washington, DC: DOC OIG.
[5] DOC OIG, July 20, 2022. *USPTO Needs to Improve Its Cost Estimating, Scheduling, and Agile Practices to Timely Retire Patent Legacy Systems*, OIG-22-026-A. Washington, DC: DOC OIG.
[6] DOC OIG, August 16, 2021. *The U.S. Census Bureau's Mishandling of a January 2020 Cybersecurity Incident Demonstrated Opportunities for Improvement*, OIG-21-034-A. Washington, DC: DOC OIG.
[7] DOC OIG, November 22, 2022. *Simulated Internal Cyber Attack Gained Control of Critical Census Bureau Systems*, OIG-23-004-I. Washington, DC: DOC OIG.
[8] FISMA has five function areas: *Identify*, *Protect*, *Detect*, *Respond*, and *Recover*. The Department increased its maturity for *Identify* and *Respond* from FY 2020 to FY 2021.

approximately 15 percent of our open investigations are pandemic related. The fraud schemes associated with our open investigations include false certifications by labs contracted to perform COVID-19 testing for the Department, false certifications and misuse of EDA-administered CARES Act and ARPA resources by revolving loan fund recipients, and misrepresentation of project eligibility for funds administered by NTIA under CAA 2021.

OIG is also pursuing four proactive initiatives around the country to identify potential fraud by recipients of pandemic funds administered by the Department. In 2022, OIG became a member of the Pandemic Response Accountability Committee Task Force, joining 14 other OIGs in providing investigative resources to pursue fraud related to various pandemic programs, including the Paycheck Protection Program and the Economic Injury Disaster Loan program.

Lessons Learned and Best Practices for Oversight

The diverse mission and broad reach of the Department of Commerce, as well as recent funding initiatives, often put Commerce OIG at the forefront of developing plans and tactics for effective oversight in a challenging environment. I would like to take a few minutes to highlight some of what we have learned over the past few years.

Oversight of Contract and Grant Programs

Since the vast majority of the Department's budget goes toward contracts and grants—especially considering the funding infusions from CHIPS, IIJA, and pandemic relief programs—OIG has long identified improving contract and grant management as a top challenge.

OIG's audit work continues to identify vulnerabilities in how the Department manages contracts and grants. In June 2020, we issued a management alert outlining the top challenges the Department would face in ensuring pandemic funds were spent timely and appropriately. The challenges we identified included:

1. Addressing ongoing disaster relief fund oversight challenges facing EDA and the National Oceanic and Atmospheric Administration (NOAA) National Marine Fisheries Service.
2. Developing and maintaining a competent acquisition and grants workforce to support the implementation and oversight of CARES Act funds.
3. Improving processes to award and monitor contracts and grants.
4. Improving control of contract and grant file management.
5. Mitigating the risk of fraud, waste, and abuse created by the significant influx of funds that need to be distributed quickly.

The use of pandemic-related funds provides a strong foundation for understanding the challenges the Department may face in administering other contract and grant programs, such as those related to the CHIPS Act and IIJA. It is important for the Department to plan for mitigation of these challenges as part of the implementation of new programs that involve an influx of funds.

Additionally, we know that fraud by contractors and grantees poses a significant risk. This focus area has become OIG's highest investigative priority. Before FY 2021, contract and grant fraud investigations accounted for 35 to 40 percent of OIG's open cases; they now account for approximately 65 percent. Recognizing the increased risks associated with significant new funding, OIG is also proactively providing guidance to the Department on how it can better prevent and detect contract and grant fraud prior to the actual distribution of funds.

Maintaining Internal Controls for Contractor-Led Programs

In addition to the challenges of administering contracts and grants, many new legislative requirements result in the Department relying on contractors' expertise to implement and operate complex programs. For example, the Department of Commerce's First Responders Network Authority (FirstNet Authority) provides insights and lessons learned on the risks associated with deferring too much to an outside entity. I will summarize three recent OIG reports that delve into these risks in further detail.

In the first report,[9] we found that FirstNet Authority did not follow GAO's Cost Estimating and Assessment Guide when preparing and documenting independent government cost estimates (IGCEs) used to evaluate its first two reinvestment proposals. Further, we found that FirstNet Authority accepted, without providing sufficient justification, AT&T's price proposals for both investments that exceeded the IGCEs by 60 percent or more.

We issued a second report[10] that found that FirstNet Authority has not established a sound process for selecting reinvestment opportunities. Specifically, we found that FirstNet Authority did not conduct a needs analysis or an analysis of alternatives, nor did it sufficiently justify the need in the business case analysis. We found FirstNet Authority relied on contractor information that appeared to influence the process of identifying and selecting reinvestment opportunities. A more effective evaluation process would help FirstNet Authority:

1. determine which investment opportunities are most beneficial;
2. determine which should be prioritized for maximum benefits to public safety; and
3. ensure funds are spent efficiently.

We made recommendations to improve the reinvestment process that could put more than $296 million in funds to better use and ensure future multibillion-dollar reinvestments are supported and justified and reflect public safety priorities.

Ensuring appropriate task order oversight is one of FirstNet Authority's FY 2023 top management challenges. Our recent audit of the oversight of the first two initial task orders addressed this challenge.[11] On March 1, 2023, OIG reported findings that:

[9] DOC OIG, August 25, 2022. *FirstNet Authority Did Not Have Reliable Cost Estimates to Ensure It Awarded Two Reinvestment Task Orders at Fair and Reasonable Prices*, OIG-22-029-A. Washington DC: DOC OIG.
[10] DOC OIG, November 28, 2022, *FirstNet Authority Could Not Demonstrate Investment Decisions Were the Best Use of Reinvestment Funds or Maximized the Benefits to Public Safety*, OIG-23-005-A. Washington DC: DOC OIG.
[11] DOC OIG, March 1, 2023, *FirstNet Authority Failed to Provide Adequate Contract Oversight for Its Initial Two Reinvestment Task Orders,* OIG-23-012-A. Washington DC: DOC OIG.

1. FirstNet Authority did not have sufficient performance measurements in the Quality Assurance Surveillance Plan to adequately assess contractor performance for its first two reinvestment task orders;
2. FirstNet Authority did not perform independent verification of contractor performance regarding deployables;
3. FirstNet Authority contracting officer's representatives relied on Nationwide Public Safety Broadband Network (NPSBN) Program Management Office personnel that were not certified or formally appointed to conduct contract monitoring; and
4. FirstNet Authority's Senior Management Council reviews were not conducted in a transparent manner for the NPSBN reinvestment TOs.

These examples demonstrate the risks the Department faces when it is necessary to rely heavily on a contractor to implement new programs. Commerce OIG used the lessons learned from these examples and our other work to inform the challenges we identified for CHIPS Act and IIJA implementation. Our work has shown that when implementing programs of a complex and technical nature (such as CHIPS Act programs), the Department must maintain continuous, stringent oversight and independence to ensure the objectives of the program are achieved and that contracts bring maximum value for the Department and taxpayers.

OIG Culture and Improvements

The Department of Commerce remains on the forefront of innovation and advances that are important for the country, particularly with the leadership and implementation of the CHIPS Act and IIJA. While providing oversight to the Department's activities in these areas will be a complex task, I am confident that Commerce OIG is ready to meet the challenge. In addition to the lessons learned I have just cited, which give us insight into the risks associated with these programs, I have implemented numerous cultural and operational improvements that position OIG to succeed. I am proud of the work OIG does and the people that make it all happen.

Improvements to OIG's Operations and Employee Satisfaction

When I assumed the duties of IG at Commerce, I walked into a difficult situation. Morale was extremely low. Turnover was extremely high. The office had a high degree of dysfunction, particularly within its leadership ranks. Today, the environment is much different, thanks to a massive transformation we have brought about. The following are among our many accomplishments over the past few years:

- We have improved our audit processes and our report review process. The quality of our audit products has risen and stayed high.
- Our HR office has consistently ranked among the top servicing HR offices in the Department of Commerce. We are proud to hire a greater percentage of veterans than any other entity in the Department.
- Our Office of the Chief Information Officer has completely turned around what was a poorly performing network and now leads the Department in many ways.

- Our CFO adeptly manages our budget every year, and we efficiently use all funding.
- Federal Employee Viewpoint Survey scores tell us that morale has risen and stayed high.
- In the two most recent Best Places to Work rankings, OIG's scores in the overall engagement index rose 29.6 points to the highest scores ever for this OIG. The scores rose more than for any other OIG in the rankings.
- The Best Places to Work index that deals with effective leadership has likewise reached its highest scores ever, increasing by 28.9 points in 2 years.
- We were ranked number one of all OIGs in the new Employee Well-Being Index, scoring 97.6.
- Our recruiting is the best it has ever been. We attract highly skilled and experienced candidates. We hire them quickly, and we retain them. We are in our fourth year of very low employee turnover.

One of the main drivers of success has been our emphasis on communication, with 93 percent of OIG employees rating internal communication from leaders as effective. We are very open to input from employees, we tell our employees what we are doing and why, we work to make sure they know what is going on throughout the organization, and we recognize and celebrate excellent performance.

Improvements to the Office of Investigations

I would also like to highlight specific improvements to how OIG's Office of Investigations operates. First, since FY 2020 we have doubled its staff, from 19 employees to 40. We have reshaped the office to include a division that provides training and support for all of our investigators. We also created a headquarters investigative team that focuses on whistleblower retaliation investigations, senior level employee misconduct, and hotline triage, while allowing the Investigative Operations Division to focus on high-impact contract and grant fraud investigations.

We have made a concerted effort to refocus investigative capabilities and priorities on the most vulnerable programs with the greatest impact for the Department and taxpayers.

We have also shifted the culture from relying on hotline complaints to being a proactive investigative team, including:

- conducting outreach and providing fraud awareness training to government personnel, contractors, grantees, and subrecipients so they know what and how to report fraud;
- conducting outreach with the Department of Justice, other OIGs, partner law enforcement agencies, and state and local oversight agencies around the country to make them aware of our mission and investigative interests;
- applying algorithms for fraud indicators to use in analysis and data mining;
- leveraging audits and auditors, who are often in position to identify fraud indicators; and

- partnering with the Department to implement antifraud measures into contract and grant requirements before funds are distributed.

We have already seen results from this shift to proactivity:

- Cases opened based solely on analysis and investigator efforts increased from just 2 percent of total cases in FY 2019 to 37 percent in FY 2022.
- Cases opened based on analysis, investigator efforts, liaison, and audit referrals jumped from 6 percent in FY 2019 to nearly 60 percent thus far in FY 2023.

Conclusion

The overall effect of the improvements made to OIG culture is that we stand ready to tackle the toughest challenges. We are grateful for Congressional support and funding that allows us to deploy our resources to the highest priority areas. I am committed to maintaining a workforce that can drive improvements to the programs and operations of the Department of Commerce through independent and objective oversight. I am grateful for the opportunity to testify here today, and I welcome any questions you may have.

Peggy E. Gustafson

Peggy E. (Peg) Gustafson was sworn in as Inspector General of the U.S. Department of Commerce on January 9, 2017. Peg was nominated by the President in March 2016 and confirmed by the Senate on December 10, 2016. Peg leads a team of auditors, investigators, attorneys, and support staff responsible for reviewing and improving the Department's business, scientific, economic, and environmental programs and operations.

Before assuming her current post, Peg was the Inspector General of the U.S. Small Business Administration, a position she had held since October 2009. She previously served as General Counsel to Claire McCaskill (D-MO), where she advised the Senator on government oversight issues and helped write two bills that have significantly strengthened the federal offices of Inspectors General: the Inspector General Reform Act of 2008 and the legislation that strengthened the office of Special Inspector General for the Troubled Asset Relief Program.

During her tenure as Chair of the Legislation Committee for the Council of Inspectors General on Integrity and Efficiency, Peg worked with lawmakers on legislation to ensure the continued independence of Inspectors General, including the Inspector General Empowerment Act of 2016, which passed Congress and was signed into law in December 2016.

From 1999 to 2007, Peg served as General Counsel in the Missouri State Auditor's Office. In that capacity, she worked closely with the auditors on issues of the scope of their duties, their need to access records, and all other legal issues arising in the course of the audits. She also served as an assistant prosecuting attorney for Jackson County, Missouri, serving as the Chair of the Insurance Fraud Task Force, and as an assistant county counselor for Jackson County.

A native of Chicago, Illinois, Peg received her B.A. from Grinnell College in Grinnell, Iowa, in 1989, and her Juris Doctor from Northwestern University in Chicago in 1992.