



**OFFICE OF INSPECTOR GENERAL**  
**U.S. Department of Energy**



**Management Challenges at  
the Department of Energy —  
Fiscal Year 2024**

DOE-OIG-24-05

November 2023



**Department of Energy**  
Washington, DC 20585

November 17, 2023

MEMORANDUM FOR THE SECRETARY OF ENERGY

SUBJECT: INFORMATION: Special Report on Management Challenges at the Department of Energy — Fiscal Year 2024

The Office of Inspector General (OIG) is required by statute to annually identify what it considers to be the most significant management challenges facing the Department. It will come as no surprise that the attached report focuses on the unprecedented challenges raised by the passage of the Infrastructure Investment and Jobs Act, the Inflation Reduction Act, the CHIPS and Science Act, and the Puerto Rico Energy Resilience Fund. Preventing fraud, waste, and abuse in connection with these funds will be extremely difficult. For this reason, I am seeking your personal support for my request to Congress that the OIG be provided \$264.7 million during the fiscal year 2024 budget cycle to perform its statutory mission in connection with these critical pieces of legislation. These funds may be provided via Congressional authorization for you to transfer such funds, or via a new appropriation.

These funds are in addition to the \$165.2 million needed to correct the historic shortfall in the OIG's base budget. The \$165.2 million is necessary for the OIG to conduct oversight of the Department's critical preexisting mission areas such as maintaining the safety and reliability of the nuclear stockpile, contract and grant administration, research security, intelligence and counterintelligence, and environmental matters.

A handwritten signature in cursive script, appearing to read "Teri L. Donaldson".

Teri L. Donaldson  
Inspector General

cc: Deputy Secretary  
Chief of Staff  
Under Secretary for Science and Innovation  
Under Secretary for Infrastructure  
Under Secretary for Nuclear Security and Administrator, National Nuclear Security Administration  
Chief Information Officer  
Deputy Chief Financial Officer

# Table of Contents

---

<u>I. Unprecedented Challenges Under Recent Legislation.....</u>	1
Overseeing the Department of Energy’s Expanded Mission — The Infrastructure Investment and Jobs Act, CHIPS and Science Act, Inflation Reduction Act, and Puerto Rico Energy Resilience Fund	
<u>II. Opportunities to Improve the Department’s Use of Technology .....</u>	3
Strengthening Cybersecurity — Protecting Sensitive Data, Information Systems, National Security, and Critical National Infrastructure .....	3
Combating the Theft of Intellectual Property — Research Security .....	7
Modernizing Oversight and Management — Access to Data for the Purpose of Running Data Analytics.....	9
Cooperation with the Office of Inspector General to Advance the Use of Technology — Successes and Failures .....	12
Developing and Deploying Artificial Intelligence — Artificial Intelligence and Technology Office .....	15
<u>III. Status of Other Management Challenges Addressed in Previous Reports .....</u>	18
Restoring Plutonium Pit Production Capability — National Nuclear Security Administration .....	18
Managing Radioactive Liquid Waste — Office of Environmental Management .....	21
Building a Stronger Suspension and Debarment Program — Upcoming Special Project Report.....	25
Improving Mandatory Disclosure Reporting — Upcoming Special Project Report.....	26
<u>Appendix: Statement of The Honorable Teri L. Donaldson, Inspector General, U.S. Department of Energy before the U.S. Senate Committee on Energy and Natural Resources, October 19, 2023.....</u>	27

# UNPRECEDENTED CHALLENGES UNDER RECENT LEGISLATION

## Overseeing the Department's Expanded Mission — The Infrastructure and Investment Jobs Act, CHIPS and Science Act, Inflation Reduction Act, and Puerto Rico Energy Resilience Fund

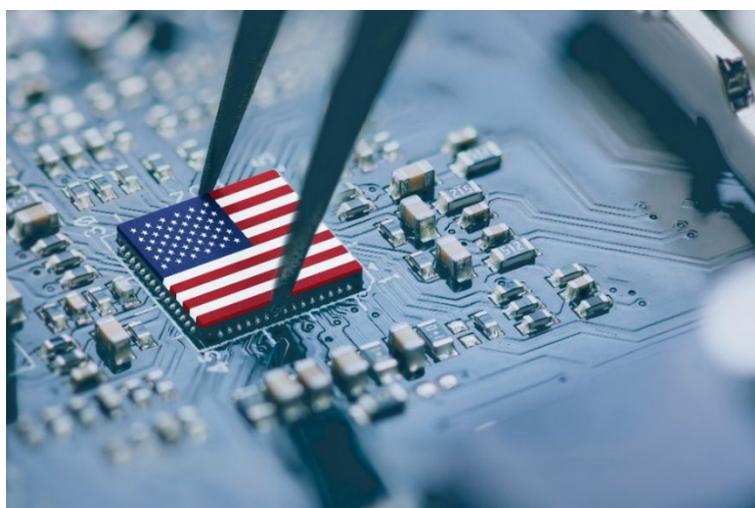


Photo courtesy of Shutterstock.com, 2023

*“Given the scope and magnitude of the Department’s responsibility in implementing the BIL and IRA, it is more critical than ever for DOE to conduct stringent oversight of program design and implementation.”*

– Dr. Kathleen Hogan,  
Department of Energy Principal  
Deputy Undersecretary for  
Infrastructure

In the past 2 years, Congress passed the Infrastructure Investment and Jobs Act (IIJA), CHIPS and Science Act (CHIPS Act), Inflation Reduction Act (IRA), and Puerto Rico Energy Resilience Fund, which collectively provided the Department with an unprecedented \$99 billion in new appropriations, \$30.5 billion in new authorizations, and an enhanced loan authority of over \$400 billion.

The current situation brings tremendous risk to the taxpayers—the combination of standing up 72 new Department programs, a real risk of funding entities owned or controlled by foreign adversaries, and a historic expansion of the Department’s loan program. As you know, these loan packages are on an accelerated schedule. One category of loan guarantees worth an estimated \$250 billion will expire on September 30, 2026. Another category of loan guarantees worth an estimated \$40 billion will expire on the same date—\$290 billion over the next 3 years or, put another way, roughly \$8 billion per month over the next 36 months. There is no precedent in the Department for this level and pace of financing. To put that amount into perspective, Wells Fargo, one of the Nation’s largest banks, had an outstanding domestic

commercial and industrial loan balance of \$292 billion as of the end of 2022.<sup>1</sup> Further, many of these projects are designed to promote innovation by financing projects not otherwise acceptable by private equity investors—projects the markets do not view acceptable.

These massive new risks to the taxpayer are occurring in tandem with substantial underfunding of the Office of Inspector General (OIG). Underfunding oversight makes an inherently risky situation much more amenable to fraud, waste, and abuse. Without substantially increased resources, the OIG’s oversight will be a fraction of what it should be, and it will not include any oversight of many key areas. Moreover, the OIG will not be able to provide the near-term audit and inspection assistance that the President specifically requested to minimize the longer-term impacts from the large-scale frauds that often plague Federal programs that provide such funding on an expediated timeline. The current level of OIG funding for oversight is both inadequate and irresponsible.

Additionally, without proper funding, critical pre-existing risk areas such as research security, contracting and payment integrity, stockpile stewardship, environmental cleanup, and pit production—to name a few—will not receive appropriate OIG oversight.

As the Pandemic Response Accountability Committee (PRAC) continues to identify the billions and billions of dollars lost or stolen from the pandemic-related Federal funding programs, there are lessons to be learned. Earlier this year, PRAC chairman Michael Horowitz testified about the use of over 69,000 questionable social security numbers to obtain \$5.4 billion in fraudulent pandemic loans and grants.<sup>2</sup> PRAC estimates a total of \$60.4 billion has been lost to fraud from the total \$655 billion in benefits provided in response to COVID-19, and other sources place that number at over \$200 billion.<sup>3</sup> Fast money must be balanced against the need for thoughtful and effective internal controls and independent audits.

During the fiscal year (FY) 2024 budget cycle, the OIG requires \$264.7 million to perform its statutory mission in connection with the IIJA, IRA, and Puerto Rico Energy Resilience Fund. This funding could be provided via a new appropriation. However, due to the spending caps enacted in the Fiscal Responsibility Act of 2023, the OIG is also requesting that Congress reallocate \$264.7 million from the Department’s unobligated balances under the IIJA, IRA, and Puerto Rico Energy Resilience Fund to provide 0.35 percent of funding in those statutes to the OIG. This can be done with no increases in appropriations.

On October 19, 2023, Department of Energy Inspector General, Teri Donaldson, testified before the Senate Committee on Energy and Natural Resources on this subject. Attached as an Appendix to this report is the complete text of Ms. Donaldson’s written statement addressing some of the many risks associated with the unprecedented increase in funding provided by these pieces of legislation.

---

<sup>1</sup> <https://www08.wellsfargomedia.com/assets/pdf/about/investor-relations/annual-reports/2022-annual-report.pdf> (p.18).

<sup>2</sup> Congressional Hearing, February 1, 2023, on Federal Pandemic Spending: A Prescription for Waste, Fraud, and Abuse (Page 3): [oversight.house.gov](https://oversight.house.gov).

<sup>3</sup> Pandemic Unemployment Insurance: How much has been paid to fraudsters?: [pandemicoversight.gov](https://pandemicoversight.gov).

# OPPORTUNITIES TO IMPROVE THE DEPARTMENT’S USE OF TECHNOLOGY

## Strengthening Cybersecurity — Protecting Sensitive Data, Information Systems, National Security, and Critical National Infrastructure

*“Our Nation is under a constant and ever-increasing threat from malicious cyber actors [...] Any disruption, corruption, or dysfunction of our vital infrastructure can have a debilitating effect on national and economic security, public health, and our everyday safety.”*

— Joseph R. Biden Jr.,  
President of the U.S.



Photo courtesy of Shutterstock, 2023

### Significance of the Issue – Cybersecurity

The Department generates and maintains some of the Federal Government’s most attractive assets to foreign adversaries, ranging from national security information to highly valuable research conducted to support both national and international goals. The Department is responsible for maintaining the Nation’s nuclear deterrent, reducing the threat of nuclear proliferation, overseeing the Nation’s energy supply, and generating cutting-edge science and technologies within its National Laboratories.

Cybersecurity is a crucial aspect of the Department’s overall security posture. While the usual attacks by adversaries remain persistent challenges, threats are increasingly coming from state-

sponsored military and intelligence organizations, terrorist groups, and international crime organizations. For example, recent reports have highlighted the increase in attacks on Federal organizations including agencies and military installations by state-sponsored adversaries, which could lead to devastating consequences in the event of a cyber breach.

### Department Progress

The Department is currently developing an agency-wide cybersecurity strategy, which the Department will use to help carry out its mandated cybersecurity responsibilities and address evolving Department and energy sector cybersecurity needs. In March 2023, the Secretary issued a memorandum directing the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) to lead cybersecurity plan coordination across program offices managing relevant provisions of the IIJA. CESER, in consultation with program offices, identified 44 provisions that it recommends be required in cybersecurity plans used by IIJA recipients. The Department also reports that it has implemented various mechanisms to allow cybersecurity-related collaboration across the enterprise and with international partners. For example, the Office of the Chief Information Officer (OCIO) staged its Cybersecurity and Technology Innovation Conference where various topics were discussed, including risks associated with the Nation's power grid. The National Laboratories also continue to collaborate on cybersecurity through various conferences and the National Laboratory Chief Information Officer Council. The Department also reports that cybersecurity continues to be a point of emphasis discussed by various working groups such as the Information Management Governance Board and the DOE Cyber and Information Technology/Operational Technology Executive Cyber and IT Council. Lastly, the Department reports engaging with industry and international partners to help drive technical collaboration in cyber and physical security of energy infrastructure to respond to emerging threats from adversaries and a rapidly changing climate.

### Challenges

The Department continues to experience many challenges related to the implementation of an effective cybersecurity program. The Department's existing governance structure continues to inhibit its ability to respond to cybersecurity evolving risks and mandates. While the Department has a Chief Information Officer (CIO) with broad responsibilities, the Department's decentralized organizational structure may impede the CIO's ability to manage and combat cybersecurity risks facing the Department. The Department lacks a centralized organizational structure, or a federated mechanism, to oversee enterprise-level risks facing the Department, and to obtain, process, and correlate real-time cyber data. This impedes the CIO's ability to manage security across the enterprise.

In addition, the Department's governance structure has caused the agency to fall behind changing cybersecurity requirements and enhancements. Despite Department directives requiring implementation of the latest Federal cybersecurity guidance published by the National Institute of Standards and Technology, various contractors performing work on behalf of the Department

and at Department-owned facilities continue to implement and assess their cybersecurity environments against outdated requirements. Contractors have reported that contractual requirements were not communicated to them or were not timely incorporated into their contracts. Officials have also expressed concerns that lines of authority have not been clear. Some sites are taking cybersecurity direction from the site offices overseeing them, but not taking direction from the OCIO. Some site officials have also resisted CIO efforts as so-called “unfunded mandates” and continue to pursue locally focused solutions for a problem that requires an enterprise approach. This type of dysfunction results in gaps and seams, duplicative investment, and friction that could put sensitive and potentially classified information at risk.

The Department has also been challenged to implement the various aspects of Executive Order (EO) 14028, *Improving the Nation’s Cybersecurity*, issued in May 2021. For instance, the EO requires agencies to advance towards implementation of a Zero Trust Architecture to improve cybersecurity, visibility, and controls, among other things. While the Department has initiated Zero Trust Architecture actions in response to the EO, much work is needed. The EO required the Department to adopt multi-factor authentication and encryption of data at rest within 180 days of the Order. However, recent correspondence from the Administration to agencies indicated a lack of progress related to these key areas of the EO. Finally, the EO directed agencies to centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks. However, the Department continues to be challenged with obtaining close to or real-time authoritative data, in particular from its management and operating and prime contractors, which impacts its ability to detect and respond to threats in a timely manner across the entire enterprise. Instead of having real-time or close to real-time data feeds from the various networks and systems supporting the Department’s mission, it relies heavily on data calls, which are prone to errors and inconsistencies, to obtain information on the sites’ security posture. The Department could substantially benefit from working toward establishing common minimum standards for a taxonomy for its cybersecurity information and leveraging sources of network information to conduct cyber analytics at the enterprise level. By performing cyber analytics at the enterprise-level, the Department would gain more visibility for making risk-based decisions and would be able to use the data to help prioritize the use of limited resources.

Another related challenge impacting the Department’s ability to enhance its cybersecurity posture is the ability to obtain adequate resources. With the addition of Federal mandates, evolving threats that require the need for better tools, and shortages in the cyber workforce, the Department must continually reprioritize its investments to ensure that its systems and data are secure. Officials have indicated that while new mandates are being established and are required to be implemented, in many cases they are underfunded or not funded at all. Further, in some cases Department programs and sites need funding to close recommendations issued by the OIG. However, officials are faced with harder-than-ever choices between addressing cybersecurity weaknesses or conducting mission-specific work, such as environmental clean-up, reducing the threat of nuclear proliferation, or conducting research at one of the many National Laboratories. This challenge was evident in our report on the *Department of Energy’s Unclassified Cybersecurity Program - 2022*, which noted that the Department was unable to fully address 38 of 61 (62 percent) recommendations made by the OIG in the prior year. This challenge could be

addressed using authoritative data driving data analytics to identify and buy down the highest risks across the enterprise, while setting conditions to further drive down costs and risks by accelerating organizational learning and reuse of leading solutions.

While the OIG's FY 2023 evaluation is ongoing, we continue to find weaknesses similar in type and frequency across the Department. Resource challenges will continue to be exacerbated by the Federal Government's, including the Department's, significant problems in obtaining and retaining a competent cyber workforce. Without adequate staffing of key cyber positions throughout the Department, the agency lacks the necessary personnel to detect and protect its systems, critical infrastructure, and data from the evolving cybersecurity threats. Notably, the Department has established a Cyber Workforce Working Group to help develop and implement solutions for attracting top cyber talent to the agency. However, the Department's challenges related to the cyber workforce will be exacerbated by introduction of new IJA and IRA activities to provide oversight and enforcement of stricter cybersecurity over the Nation's power grid.

We must also note that the lack of OIG resources has impacted our ability to fully evaluate the Department's cybersecurity posture and conduct assessments of high priority and/or high-risk areas, such as national security systems, high value assets, and operational technologies. In addition, the recent IJA legislation came with additional responsibilities related to cybersecurity; however, the OIG only received a small fraction of the funding needed to conduct the additional oversight.

## Combating the Theft of Intellectual Property — Research Security

*“The scale of their [China’s] hacking program, and the amount of personal and corporate data that their [China’s] hackers have stolen, is greater than every other country combined.”*

– Christopher Wray,  
Director, Federal Bureau of  
Investigations



Photo courtesy of Shutterstock, 2023

### Significance of the Issue – Theft by Foreign Adversaries

As reported in the FY 2022 Agency Financial Report, the Department supported \$14.8 billion in total research and development.<sup>4</sup> The risks associated with the theft of intellectual property will only increase as the Department continues to invest heavily utilizing funds under the IJJA, CHIPS Act, and IRA. While some of this work is for fundamental research that is freely published in public, much of it is subject to intellectual property protections and/or national security considerations. These major investments remain a target for foreign governments seeking to illicitly acquire access to U.S.-funded research and technologies. This is particularly troubling given the Department’s integral role in the development and maintenance of nuclear weapons systems, along with other pivotal national security missions. The economic and scientific value of the research and intellectual property developed within the Department’s complex has led foreign governments and their proxies to intensify efforts to extract information from the Department’s institutions.

### Department Progress

Since our FY 2023 Management Challenges report, the Department’s Research, Technology and Economic Security Working Group has adopted a new conflict of interest policy, released via a Financial Assistance Letter, which emphasizes combating financial conflicts of interest among Department-funded researchers, and has begun codifying this through the rulemaking

<sup>4</sup> <https://www.energy.gov/cfo/articles/fy-2022-doe-agency-financial-report>.

process. The Department has also continued work on a new conflict of commitment policy which seeks to address the same concerns for non-financial, overlapping commitments from multiple institutions that will help enhance integrity among our grantees. The Department has begun to demonstrate a commitment to preventing theft of its intellectual property by instituting prohibitions on affiliation with foreign talent programs from countries of concern for all prospective IJA funding recipients, and by signaling it will widen such restrictions to all financial assistance recipients for future funding opportunity announcements. The Department has also established a pilot Research, Technology, and Economic Security Vetting Center to support due diligence reviews in support of research, development, demonstration, and deployment activities to inform the Department of the potential risks to national security, economic competitiveness, and U.S. technological leadership.

### Challenges

While some efforts are underway, the Department must prioritize these efforts, complete these and other tasks, and ensure that it has adequate tools and resources to effectively prevent theft of intellectual property. At the same time, these tools must be designed with sufficient clarity to facilitate timely investigations and prosecutions of individuals violating the laws intended to protect this research. For example, the challenge remains in FY 2024 for the Department to fully implement National Security Presidential Memorandum 33 by creating a standardized set of required certifications and disclosures for all funding applicants. This is especially important given the significant increase in grant funds allocated under the IJA, CHIPS Act, and IRA. The Department must closely monitor the effective implementation of Department directives restricting employees and contractors from affiliating with any foreign state-sponsored programs from identified countries of concern.

Aside from such affiliations, the Department must also design requirements to deter and penalize individuals who have stolen valuable intellectual property owned by the U.S. and transported that property to our adversaries. The Department must ascribe resources to the Vetting Center to be able to effectively pursue its mission of proactively detecting foreign threats to our advanced technologies and strategic supply chains utilizing risk-based analytic tools and partnerships between program offices.

Given the importance of and risk associated with this topic, our Office of Inspections, Intelligence Oversight, and Special Projects has recently begun an inspection focusing on the Department's compliance with requirements of Department Order 486.1A, *Foreign Government Sponsored or Affiliated Activities*. The Order prohibits Department employees and contractors from participating in foreign government-sponsored talent recruitment programs and restricts other foreign government-sponsored or affiliated activities of a "foreign country of risk." Additionally, the Office of Inspections, Intelligence Oversight, and Special Projects is planning a joint project with the OIG of the Intelligence Community in FY 2024 to evaluate Department security processes in accordance with the requirements in Security Executive Agent Directives and Department Orders.

## Modernizing Oversight and Management — Access to Data for the Purpose of Running Data Analytics

*“You can have all of the fancy tools, but if [your] data quality is not good, you’re nowhere.”*

– Veda Bawo,  
Director of Data Governance,  
Raymond James



Photo courtesy of Shutterstock, 2023

### Significance of the Issue – Data Analytics

The significance of the potential use of data analytics within the Department cannot be overstated. The use of data analytics would improve effective and efficient management and oversight of the significant influx of funds associated with the IIJA, CHIPS Act, IRA, and Puerto Rico Energy Resilience Fund. It would further provide key support for the Department integrating authoritative data and data analytics into its management and oversight of its programs and operations, supporting the Department to reduce risk and support resolving its 33-year tenure on the General Accountability Office’s (GAO) High-Risk List.

### Department Progress

The Department has not kept pace with the Federal requirements pertaining to the use of data analytics. In fact, the Department is still in the early stages despite over 10 years of Congressional direction on this subject. In March 2020, the Payment Integrity Information Act of 2019 was enacted and incorporated select provisions from the Fraud Reduction and Data Analytics Act of 2015, the Improper Payments Information Act of 2002, the Improper Payments Elimination and Recovery Act of 2010, and the Improper Payments Elimination and Recovery Improvement Act of 2012 into a single subchapter in the U.S. Code. In addition, there are numerous other requirements that make up the legal framework related to the use of data analytics. For example, the 2019 Foundations of Evidence-based Policymaking Act and Federal Data Strategy published by the Office of Management and Budget (OMB), and subsequent OMB amplifying guidance and action plans, have set a comprehensive framework of internal controls for key data management, data quality, and data science requirements. These leading practices are further amplified in the GAO’s report, *A Framework for Managing Fraud Risks in Federal Programs*, issued in 2015.

The Department has taken only preliminary steps toward using data analytics in its operations. For instance, to comply with the Payment Integrity Information Act of 2019, the Department has undertaken the development and implementation of a Fraud Risk and Data Analytics Framework (Framework). Officials have defined the Framework and its placement within the organization and established a leadership hierarchy to guide the effort. To assist in the continued Framework implementation, the Department established a Senior Assessment Team to provide a leadership role in reviewing the Department's fraud risk profile and direct mitigation strategies with the support of the Data Analytics Working Group.

The Department also formed a Fraud Risk Working Group that supports preparation of the annual agency fraud risk register and fraud risk profile. The working group developed a fraud risk register based on reported fraud risks, fraud risk occurrences, and internal control entity assessment data. The register was then prioritized to prepare the Department's Fraud Risk Profile. The Department's Data Analytics Working Group also collaborated with field and contractor staff to identify contractor conflicts of interest and available data sets that could be used as pilots for data analytic purposes. Finally, the Department has recently onboarded a new Chief Data Officer, with scope and responsibilities as outlined in the 2019 Foundations of Evidence-based Policymaking Act.

### Challenges

While planning is very important, it is not a substitute for making operational progress. Many challenges remain. For instance, the IRA provided the Department funding for three rebate programs which will be administered by the Department's Office of State and Community Energy Programs. Initial efforts by the OIG, to be developed and published via an upcoming report, have identified shortfalls in the data being collected by recipients and a lack of information being shared across recipients, reflecting risks that could hamper the identification and prevention of fraud. Further, our prior reports on the Department's Payment Integrity Reporting in its annual agency financial report have noted that the Department could increase its use of data analytics that would allow it to move away from pay and chase toward prevention, which is a more efficient and accurate method of identifying improper payments. Additionally, a 2022 survey conducted by the Department to establish a baseline of data analytics capabilities being performed Department-wide identified widespread data literacy shortcomings across the reporting entities and found that the practice of data analytics is inconsistent and underdeveloped across the complex. For example, data analytics capabilities at some reporting entities consisted primarily of maintaining spreadsheets and manual reconciliation efforts.

The Department is also lagging on completion and integration of actions outlined in the Federal Data Strategy action plans, such as those related to establishing a framework for data management, data governance, establishing an enterprise data catalog, and assessing data management maturity.

Another significant challenge the Department faces is identifying the data systems and sources used by the Department and its contractors. While the OCIO attempted to document the data analytics activities being performed by Department elements and the data systems in use during the past year, the results of the effort were not sufficient or even usable. Further, even when systems are identified, the Department may encounter challenges accessing data, especially for systems managed by its contractors.

The OIG will soon be issuing a Special Project Report on the Department's underutilization of data analytics, and the dangers of continuing to underutilize this powerful tool.

## Cooperation with the Office of Inspector General to Advance the Use of Technology — Successes and Failures

### Successes

The Department has cooperated with the OIG's efforts to assess and improve the Department's cybersecurity posture. As a result of this cooperation, the OIG has identified over 44,000 cybersecurity vulnerabilities across 13 sites, and the Department has acted to address many of the vulnerabilities identified.

### Failures

The Department has not fully cooperated with the OIG's efforts to collect information needed to utilize data analytics to protect the Department against fraud, waste, and abuse.

In September 2021, the OIG requested payroll-related records from one Department contractor for the purpose of conducting data analytics to help identify potential fraud by contractors who work onsite at Department laboratories, including its nuclear laboratories and other Department facilities. This contractor cooperated with the OIG and provided the requested data in a timely manner within 45 days. The OIG has since analyzed that data and uncovered numerous fraudulent activities, resulting in several active criminal investigations and indictments.

Additionally, the OIG acquired the same payroll-related data for groups of Department Federal employees, and the Department cooperated with these efforts. The OIG is currently analyzing that data and has already uncovered additional potentially fraudulent activities.

It is vitally important for the Department to be able to timely identify potential wrongdoing by individuals working in the agency's highly sensitive facilities, whether those individuals are employed by the Department directly or by one of its contractors. In addition to protecting the existing mission elements of the Department from the obvious risks of employing criminals, identifying and prosecuting these individuals is an obvious first step to protect the Department's new mission elements being funded at unprecedented levels under the IIJA, IRA, and Puerto Rico Energy Resilience Fund.

Data analytics is the most efficient and powerful tool to utilize for helping to ensure the integrity of the Department's workforce, and to timely identify any wrongdoing. For this reason, in March 2022, the OIG issued similar payroll-related data requests to 10 contractors at 5 Department sites.

For over a year, the Department did not timely comply or support the OIG's efforts to collect this data from the 10 contractors on the grounds that the contractors had advised that they would

refuse to provide it. Bottom line—the Department declined to acknowledge, much less enforce, the contractual obligation of these contractors to cooperate with the OIG.

On May 12, 2023, the Inspector General elevated this matter to the Secretary at a meeting, also attended by the Deputy Secretary, the National Nuclear Security Administration (NNSA) Administrator, and the General Counsels for both the Department and NNSA. Although the Inspector General was under no legal obligation to do so, she deferred one of the items on the list, with the understanding that the OIG may later request the remaining item once the OIG has an opportunity to review the other requested information. The Inspector General deferred this single item with the understanding that the additional categories of data would be provided to the OIG.

For the next 6 months, the Department did not request the data from its contractors. Instead of enforcing its own contractual obligations, the Department provided the OIG with incomplete and unusable employee data maintained by the General Services Administration. During the course of these protracted discussions with the Department, the OIG discovered a very troubling fact: the Department does not maintain the most basic data that would allow the Department to identify the individuals working within the Department’s government-owned and often highly sensitive facilities. This fact raises serious security concerns.

In any case, the Department long ago acknowledged that it may request such identifying data from these contractors, all of which are operating federally owned facilities. However, as of the end of September 2023, the Department had declined to do so in any comprehensive way.

On October 5, 2023, the Department requested that a single contractor provide the data to the OIG within 30 days. That contractor provided data on November 3, 2023. Based on the OIG’s preliminary review of this data, it appears to be largely complete. The OIG will continue to work with this contractor to complete the production.

On November 13, 2023, the Department requested that a second contractor provide the data to the OIG within 30 days.

On November 14, 2023, the Department directed that six additional contractors provide the data to the OIG within 30 days.

Also, on November 14, 2023, the Deputy Secretary informed the OIG that NNSA will be directing the last two of the contractors to provide the data.

Once the remaining data is provided, the OIG will review it and work directly with the contractors to discuss any deficiencies.

As a result of the Department's failure to timely cooperate with our oversight work, the OIG is reporting this in our *Semiannual Report to Congress* as restricted/significantly delayed access to records. Additionally, the OIG intends to issue a Special Project Report on this subject in December of 2023.

## Developing and Deploying Artificial Intelligence — Artificial Intelligence and Technology Office



Photo courtesy of Shutterstock.com, 2023

*“Advances in AI are enabling enormous progress and breakthroughs that can help address key challenges of our time [...] at the same time [...] widespread AI access also carries unprecedented risks.”*

– David M. Turk,  
Deputy Secretary of  
Energy

### Significance of the Issue – Artificial Intelligence

The past year witnessed an explosion in interest regarding artificial intelligence (AI), machine learning, and large language models. The interest engenders both optimism about AI’s ability to solve problems as well as concerns about AI’s role in everyday life, including ensuring relevant security and ethical concerns are appropriately considered. AI also has the potential to transform many aspects of discovery and applied technology and science; manufacturing, infrastructure, finance, and commerce; Government operations; and national security.

On October 30, 2023, the President issued EO 14110, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, emphasizing the critical need for the Federal Government to immediately attend to these issues.

With its research capabilities, the Department has a tremendous opportunity to provide leadership covering research principles and guidelines, processes, and technical rigor. As the custodians of the most advanced high-performance supercomputers and massive multimodal data sets stemming from diverse research, the Department and its National Laboratories are well-situated to collaborate with each other and external partners in taking a leading role in developing and deploying AI. There is no doubt that AI properly deployed would also enhance the Department’s own operations.

## Department Progress

In February 2019, December 2020, and October 2023, the President promulgated the EO directing the Department and other Federal agencies to pursue strategic objectives to promote and protect American advancements in AI. These objectives include, among others: sustained investment in AI research and development in collaboration with industry; enhanced access to high-quality and fully traceable Federal data, models, and computing resources; and minimized vulnerability to AI-enabled attacks from malicious actors. EO 13859, *Maintaining American Leadership in Artificial Intelligence*, states that leadership in AI will require a “whole-of-government approach” that will include meaningful contributions from Department and other Federal agencies working in partnership with experts in the private and academic sectors. In particular, EO 13859 states:

Maintaining American leadership in AI requires a concerted effort to promote advancements in technology and innovation, while protecting American technology, economic and national security, civil liberties, privacy, and American values and enhancing international and industry collaboration with foreign partners and allies.

EO 13960, *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*, established guidelines and principles for the use of AI within the Federal Government. It focused on ensuring that AI technologies are reliable, transparent, and secure.

On October 30, 2023, the President issued EO 14110, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*. This EO requires the Secretary to develop and implement a plan for developing the Department’s AI model evaluation tools and testbeds. The EO also requires the Secretary to take actions to support more effective enterprise-wide inventory, data, and workforce management processes surrounding the agency’s AI activities. Developing a robust enterprise data management and governance structure is necessary for the Department to achieve the responsible use of AI.

Prior to the entry of EO 14110, the Department had already set a goal of becoming a leader among Federal agencies in the development and deployment of AI technology. To do so, in September 2019 the Secretary of Energy created the Artificial Intelligence and Technology Office (AITO) to foster the strategic coordination and development of AI capabilities across the Department by serving as the central point of coordination for the broad and extensive capabilities of the Department and its National Laboratory Complex. In 2021, AITO set the goal of the Department’s civilian leadership in the use of AI. In consultation with the National Institute of Standards and Technology, AITO developed the *DOE AI Risk Management Playbook*. This is a reference guide for AI-risk identification and potential mitigations. More recently, the OCIO released its *Generative Artificial Intelligence Reference Guide* in August 2023 to provide guidance on gaining an understanding of key considerations, risks, and best practices associated with the use of generative AI. In addition, the Department’s DOE Artificial Intelligence Exchange System captured over 1,800 AI projects across the enterprise and more than 530 use cases, of which more than 180 were publicly released.

The Department also recently announced several awards to enhance AI research including:

- \$29 million for research on machine learning, AI, and data resources for fusion energy sciences;
- \$16 million for research on scientific machine learning for complex systems; and
- Berkeley National Laboratory’s Nuclear Science Division received two DOE funding awards for 2-year projects focused on AI and machine learning.

The President’s FY 2024 budget includes a request of \$730 million for cutting-edge research in AI, quantum information sciences, microelectronics, and isotope production within the Department’s Office of Science. These activities will require significant Department coordination, oversight, and direction. The Department also plans to transition the AITO into the Office of Science in FY 2024 and expand the number of employees in that office to help address emerging challenges.

### Challenges

While the Department reports making investments in AI, these advancements appear program specific and site specific. There is little enterprise level clarity on approaches, frameworks, guidelines, and policies that will be needed to govern and coordinate the AI efforts across the complex, in line with EO 13960. Without a strong governance structure in place and common minimum standards to allow for methodical management of AI issues, the Department may be unable to keep up with the fast-changing AI landscape and related ethical, security, and use concerns.

Realizing the Department’s goal of AI leadership will also require effective Department oversight to coordinate cross-cutting and enterprise-wide efforts with contributions from the Office of Science, CESER, the OCIO (including the Chief Data Officer), the Department’s National Laboratories, and NNSA. The opportunities to lead in the deployment and use of advanced AI technology will also require funding and active partnerships with industry and academia.

Currently, the Department lacks focus on specific actions or a detailed roadmap to guide its path forward. Many efforts for AI and machine learning appear to focus on broad goals and objectives without a clear plan for implementation, making it difficult to assess the Department’s commitment, metrics, and progress toward achieving its AI and machine learning goals.

Given their inter-relationship, clarifying and deconflicting AI governance and data analytics, cybersecurity, and IT governance will also be required.

# STATUS OF OTHER MANAGEMENT CHALLENGES DISCUSSED IN PREVIOUS REPORTS

## Restoring Plutonium Pit Production Capability — National Nuclear Security Administration



*“If we fail to recapitalize plutonium pit production now, we risk catastrophic failures given an infrastructure incapable of responding in a timely manner.”*

– Charles A. Richard,  
Commander, U.S. Strategic  
Command

Molten plutonium. (Source: <https://www.energy.gov/nnsa/plutonium-pit-production>)

### Significance of the Issue – Pit Production

NNSA is responsible for maintaining a safe, secure, reliable, and effective nuclear weapons stockpile. Plutonium pits are a vital component in all U.S. nuclear weapons. During the Cold War, the Nation produced more than 1,000 plutonium pits per year (ppy) at the Rocky Flats Plant in Colorado. Since the closure of the Rocky Flats Plant in 1992, the U.S. has lacked the capability to produce significant quantities of new plutonium pits. NNSA is developing the capability to manufacture plutonium pits at the rate of at least 80 war-reserve<sup>5</sup> (WR) ppy.

<sup>5</sup> WR pits have been certified to meet the stringent quality assurance requirements necessary to enter the U.S. nuclear weapons stockpile.

Maintaining confidence in the nuclear warheads that compose our Nation’s nuclear deterrent requires the Department to re-establish a plutonium pit manufacturing capability. Newly manufactured pits are required to improve warhead safety and security, mitigate the risk of erosion of confidence in the deterrent posed by plutonium/pit aging, and support potential changes to future warheads due to threats posed to the U.S. nuclear deterrent from renewed peer competition.

### Department Progress

To reach the capability to produce 80 ppy, NNSA implemented a two-site solution with the objective of producing 30 WR ppy at Los Alamos National Laboratory (LANL) at the existing Plutonium Facility-4 (PF-4), while also producing 50 WR ppy at the Savannah River Site (SRS) Savannah River Plutonium Processing Facility (SRPPF). The OIG did not perform any oversight work over the last year pertaining to this challenge area; therefore, we cannot give an opinion on the Department’s progress in this area. However, in July 2023, NNSA released a fact sheet that provided a status on its pit production effort.

According to the fact sheet, PF-4 currently has the ability to produce pits and has produced a total of 30 WR pits since 2000. However, to reach the capability of 30 WR ppy, decontamination and removal of old equipment is ongoing, which will allow for new equipment to be installed. PF-4 will continue to build pits throughout equipment removal and installation, and capacity and resilience will grow steadily over time. At the time the fact sheet was published, PF-4 expected to have its first fully qualified pit, the “first production unit,” in the second half of 2024, and it appeared that equipment installation will not be completed until sometime between late 2027 and August 2030.

At the SRS, the fact sheet stated that design efforts are currently underway for the process equipment, the glove boxes that surround the equipment, and the many systems that connect to the gloveboxes in the main processing building. Although cost and schedule for SRPPF remained uncertain at the time the fact sheet was published, NNSA has determined that producing 50 ppy by 2030 at SRS to meet the overall 80 ppy objective is not achievable. The SRPPF assessment is based on considerations that to produce WR pits at the required rate necessitates successful completion of the following three activities: (1) completing SRPPF construction and receiving startup authorization (CD-4); (2) demonstrating a WR-quality pit manufacturing capability; and (3) demonstrating the ability to manufacture at full rate capacity while maintaining WR quality control. After construction is finished, it may still take several years for this newly constructed facility to complete the testing and gain approval to enter “hot” operations. Ramping up to full rate production will also take time.

Although NNSA will not reach the capability to produce 80 ppy by the original target date of 2030, NNSA reports working with LANL and SRS to achieve this production rate as soon as possible. The fact sheet also stated that NNSA continues to communicate pit-production

schedule estimates and uncertainties to the Department of Defense and its military partners, who continue to work with NNSA to plan for a safe, secure, reliable, and effective nuclear deterrent force in the face of these uncertainties.

### Challenges

The Department faces challenges in meeting its production objectives. The U.S. ceased large-scale pit production in 1989, and as a result, most pits in the U.S. stockpile are more than 30 years old. The GAO was asked to review NNSA’s plutonium pit production activities and released a report in January 2023, *NNSA Does Not Have a Comprehensive Schedule or Cost Estimate for Pit Production Capability*. In the report, the GAO stated that “[r]establishing pit production likely represents NNSA’s largest investment in weapons production infrastructure to date” and recommended that NNSA develop a life cycle cost estimate.

In its review, the GAO found that NNSA had not developed either a comprehensive schedule or cost estimate that met GAO best practices. It found that NNSA’s schedule does not include all activities or milestones to achieve the stated 80 ppy production capability and does not assign resources to activities. An incomplete integrated master schedule increases the likelihood of disruption and delay.

## Managing Radioactive Liquid Waste — Office of Environmental Management



*“Protecting the environment by addressing radioactive waste stored in underground tanks at Hanford, Savannah River and the Idaho National Laboratory is a top priority for EM.”*

– William “Ike” White,  
Senior Advisor for the  
Office of Environmental  
Management

Inside view of waste tank AX-101 at the Hanford Site.

(Source: <https://www.energy.gov/em/articles/hanford-makes-tank-waste-retrieval-progress-aax-complex>)

### Significance of the Issue – Radioactive Liquid Waste

The Office of Environmental Management (Environmental Management) is responsible for addressing the environmental legacy of decades of nuclear weapons production and Government-sponsored nuclear energy research. This mission includes the safe, effective, and cost-efficient management, treatment, and disposition of high-level radioactive waste (i.e., “tank waste”) generated through legacy-spent nuclear fuel reprocessing and other plutonium processing activities. Environmental Management manages a total inventory of approximately 92 million gallons of tank waste, which is a primary environmental risk at most sites where it is located. At the Hanford Site (Hanford), SRS, and the Idaho National Laboratory Site (INL), the remaining tank waste is stored in aging underground tanks.

In addition to environmental risks, this waste represents a significant financial burden to the U.S. Government. The Department is the top contributor to the Federal Government’s overall environmental liabilities, with Environmental Management’s current total environmental liability approximately \$406 billion in 2021 constant dollars according to the Department’s FY 2022 Agency Financial Report.

## Department Progress

The OIG did not complete any oversight work over the last year in this area; therefore, we cannot opine on the Department's progress in this area. However, we are providing the following information obtained from the Department.

The Department has instituted new policies and approaches that have the potential to open new disposition pathways for tank waste. In FY 2019, the Department issued its interpretation of the statutory term, "high-level radioactive waste," as defined in the Atomic Energy Act of 1954, as amended, and the Nuclear Waste Policy Act of 1982, as amended. This interpretation allows for managing tank waste via its radioactive characteristics, not by how the waste was generated. The high-level radioactive waste (HLW) interpretation could enable the Department to manage and dispose of tank waste in a risk-based and more cost-effective manner that remains protective of human health and the environment more appropriately. Secretary Granholm committed to assessing the HLW interpretation during her Congressional confirmation hearing in January 2021. This assessment, which was completed in December 2021,<sup>6</sup> concluded that the HLW interpretation is consistent with the law, science and data, and the recommendations of the Blue-Ribbon Commission on America's Nuclear Future. The Department is currently in the process of evaluating a second waste stream (i.e., contaminated process equipment) at SRS for potential disposal at a licensed commercial facility under the HLW interpretation.

### Hanford

At the Hanford Waste Treatment and Immobilization Plant (WTP), startup and commissioning preparations are underway. According to a WTP Project Review, in August 2023, test glass production is scheduled to begin at the Low-Activity Waste Facility, and cold commissioning is scheduled to begin in FY 2024 to support commencement of radiological operations in 2025. Additionally, according to a Hanford June 2023 report, operations of Hanford's Tank Side Cesium Removal System has processed over 500,000 gallons of low-activity tank waste in preparation to send to the Low-Activity Waste Facility.

### SRS

Based on documentation from SRS, the Department initiated hot commissioning of the Salt Waste Processing Facility (SWPF) in October 2020 and began full operations of the facility in January 2021. Since the introduction of radioactive salt waste to the SWPF, SRS stated it has

---

<sup>6</sup> Assessment of Department of Energy's Interpretation of the Definition of High-Level Radioactive Waste, a Notice by the Department on December 21, 2021, 86 Federal Register 72220, available at <https://www.federalregister.gov/documents/2021/12/21/2021-27555/assessment-of-department-of-energys-interpretation-of-the-definition-of-high-level-radioactive-waste>.

processed over 3 million gallons of salt waste. According to SRS, as the SWPF increases efficiency and optimizes its operations, process rates of up to 6 million gallons annually are projected with current technologies.

## INL

At INL's Integrated Waste Treatment Unit (IWTU), Department officials indicated that the Department began radiological operations in April 2023 with a blend of 10 percent sodium-bearing waste and 90 percent simulant, and that in May 2023, the IWTU began treating 100 percent sodium bearing waste.

## Challenges

While progress has been made in establishing its capabilities to treat tank waste for final disposition, significant work remains.

## Hanford

The Department reports needing to identify and develop technically achievable, cost-effective, and viable approaches for treating the high-activity inventory of tank waste at Hanford for disposition. The current program of record calls for the WTP's Pretreatment and High-Level Waste facilities to prepare and vitrify the high-level waste for eventual final disposition.

Additionally, the Department reports needing to complete startup and commissioning of those facilities involved in the processing of low-activity waste. Further, the Department must identify additional treatment options to address Hanford's remaining low-activity inventory. A study, conducted by the Federally Funded Research and Development Center National Academies of Sciences, Engineering and Medicine, recommended the Department consider grout as an alternative to supplemental treatment of low-activity liquid waste. To that end, the Department is working with regulators to advance a Test Bed Initiative, in which it will treat 2,000 gallons of tank waste sufficiently for offsite immobilization in grout and disposal.

## SRS

The Department reports needing to continue improving the Defense Waste Processing Facility's and SWPF's long-term reliability and availability. According to SRS, when the Next Generation Solvent is implemented at the SWPF, it will enable processing greater than the 6 million gallons of waste per year capability provided by the original solvent. SRS also stated that to complete the bulk of the tank waste mission at SRS in the next decade, the Department will need effective management of the spent nuclear fuel processing mission at the Savannah River H-Canyon facility, which contributes to the site's tank waste mission.

## INL

Department officials at INL indicated that it will need to focus on safe operation of the IWTU and interim storage of the stainless-steel canisters until they can be permanently disposed of in a national geologic repository. According to Environmental Management's Program Plan of FY 2022, waste treatment is expected to take from 5 to 7 years to complete. Additionally, the Department will need a pathway for the disposal of the processed waste currently stored at INL.

## Building a Stronger Suspension and Debarment Program — Upcoming Special Project Report

In previous Management Challenges Reports, we identified opportunities to improve suspension and debarment processes at the Department. Suspension and debarment are the primary means the Government uses to mitigate risk from parties that have shown themselves not to be responsible participants in Federal procurements, grants, agreements, programs, and transactions. While these remedies typically rely upon criminal convictions or serious civil offenses, Suspension and Debarment Officials may impose these exclusions whenever evidence indicates that the individual or company is not presently responsible, and therefore presents a risk to Federal programs and operations. Historically, the Department has not operated a robust suspension and debarment program.

In the past 2 years, the OIG has created a special division to improve the referral process and better enable the Department to operate a more robust suspension and debarment program. As a result, the OIG has substantially increased the volume of more detailed referrals to the Department.

In December of 2023, the OIG will publish a Special Project Report on this subject. The Special Project Report will describe the OIG's overhaul of its own suspension and debarment practices and procedures and make specific recommendations to the Department for improving its oversight efforts.

## Improving Mandatory Disclosure Reporting — Upcoming Special Project Report

The Federal Acquisition Regulation’s Mandatory Disclosure Rule (MDR) contract clause requires certain Federal contractors to disclose to the OIG in a timely manner, in writing, whenever the contractor has credible evidence of violations of Federal criminal law involving fraud, conflict of interest, bribery, gratuity violations, or violations of the civil False Claims Act. Over a 2-year period, the OIG conducted inspections at several Department sites and discovered significant lapses in reporting under the MDR.

In December 2023, the OIG will publish a Special Project Report on this subject. The Special Project Report will describe the OIG’s overhaul of its own MDR practices and procedures, and make specific recommendations to the Department for improving its oversight efforts.

# APPENDIX

## Statement of The Honorable Teri L. Donaldson, Inspector General, U.S. Department of Energy before the U.S. Senate Committee on Energy and Natural Resources, October 19, 2023

U.S. Department of Energy  
Office of Inspector General

---

Statement  
of  
The Honorable Teri L. Donaldson, Inspector General  
U.S. Department of Energy

before the

U.S. Senate  
Committee on Energy and Natural Resources

October 19, 2023

## Introduction

Chairman Manchin, Ranking Member Barrasso, and members of the committee:

Thank you for inviting me to testify today on the risks arising from the major expansion of both the Department of Energy’s loan programs and its grant<sup>1</sup> programs, as funded by recent pieces of legislation which collectively appropriated \$99 billion to the Department and increased the Department’s loan authority by an estimated \$385 billion.

The current situation brings tremendous risk to the taxpayers — the combination of standing up 72 new Department programs, a real risk of funding entities with foreign ownership or control, and a historic expansion of the Department’s loan program. As you know, these loan packages are on an accelerated schedule. One category of loan guarantees worth an estimated \$250 billion will expire on September 30, 2026. Another category of loan guarantees worth an estimated \$40 billion will expire on the same date—\$290 billion over the next 3 years or, put another way, roughly \$8 billion per month over the next 36 months. There is no precedent in the Department for this level and pace of financing. To put that amount into perspective, Wells Fargo, one of the Nation’s largest banks, had an outstanding domestic commercial and industrial loan balance of \$292 billion as of the end of 2022.<sup>2</sup> Further, many of these projects are designed to promote innovation by financing projects not otherwise acceptable by private equity investors – projects the markets do not view acceptable.

These massive new risks to the taxpayer are occurring in tandem with substantial underfunding of the Office of Inspector General (OIG). Underfunding oversight makes an inherently risky situation much more amenable to fraud, waste, and abuse. Without substantially increased resources, the OIG’s oversight will be a fraction of what it should be, and it will not include any oversight of many key areas. For example, with current funding, the OIG may only be able to conduct 50 oversight projects pertaining to the \$65 billion of grant and financial assistance awards, even though we have determined that more than 400 oversight projects are necessary to protect the taxpayers. Moreover, the OIG will not be able to provide the near-term audit and inspection assistance that the President has specifically requested to minimize the longer-term impacts from the large-scale frauds that often plague Federal programs that provide such funding on an expediated timeline. The current level of OIG funding for oversight is both inadequate and irresponsible.

Additionally, without proper funding, critical pre-existing risk areas such as research security, contracting and payment integrity, stockpile stewardship, environmental cleanup, and pit production—to name a few—will not receive appropriate OIG oversight.

---

<sup>1</sup> For purposes of the document, the term “grants” includes cooperative agreements and other transactions such as direct subsidies, prize competitions, etc. Both grants and cooperative agreements deliver Federal funds to recipients. With cooperative agreements, the Federal Government may be more involved in guiding or participating in project activities.

<sup>2</sup> <https://www08.wellsfargomedia.com/assets/pdf/about/investor-relations/annual-reports/2022-annual-report.pdf> (p.18)

As the Pandemic Response Accountability Committee (PRAC) continues to identify the billions and billions of dollars lost or stolen from the pandemic related federal funding programs, there are lessons to be learned. Earlier this year, PRAC chairman Michael Horowitz testified about the use of over 69,000 questionable social security numbers to obtain \$5.4 billion in fraudulent pandemic loans and grants.<sup>3</sup> PRAC estimates a total of \$60.4 billion has been lost to fraud from the total \$655 billion in benefits provided in response to the pandemic, and other sources place that number at over \$200 billion.<sup>4</sup> Fast money must be balanced against the need for thoughtful and effective internal controls and independent audits.

Due to the spending caps proposed in the Fiscal Responsibility Act of 2023, I am recommending that Congress reallocate funds from the Department's unobligated balances under the Infrastructure Investment and Jobs Act (IIJA), Inflation Reduction Act (IRA), and Puerto Rico Energy Resilience Fund to provide 0.35 percent of funding in those statutes to the OIG. This can be done with no increases in appropriations. This makes sense. In fact, the Environmental Protection Agency has already agreed to transfer additional funds to its OIG in the same manner for the same reason.

I have asked for the administration's support of this proposal. I am here today to ask the same of this committee, and to further discuss some of the risks associated with this unprecedented influx of funding. Please support my request to be properly funded as discussions continue to finalize the fiscal year 2024 budget.

### **Recent Legislation Increased Loan Program by \$385 Billion**

Three recent legislative actions expanded existing Department authorities for loans and loan guarantees by an estimated \$385 billion. Beginning with the most recent legislation:

- The 2023 Consolidated Appropriations Act expanded the Department's loan guarantee authority by \$15 billion. This authority supports commitments to guarantee loans for eligible projects under title Title XVII of the Energy Policy Act of 2005 for Innovative Technology Loan Guarantee, Section 1703. Eligible projects must: (1) avoid, reduce, or sequester air pollutants or anthropogenic greenhouse gas emissions, and (2) employ new or significantly improved technologies. This authority does not have a statutory expiration date but is available until the appropriations for credit subsidy supporting it are expended.

---

<sup>3</sup> Congressional Hearing, February 1, 2023, on Federal Pandemic Spending: A Prescription for Waste, Fraud, and Abuse (Page 3): [oversight.house.gov](https://oversight.house.gov)

<sup>4</sup> Pandemic Unemployment Insurance: How much has been paid to fraudsters?: [pandemicoversight.gov](https://pandemicoversight.gov)

- IRA expanded the Department’s loan and loan guarantee authority up to approximately \$350 billion, covering several authorities:
  - Title XVII Innovative Technology Loan Guarantee, Section 1703, was expanded by \$40 billion and covers the same type of work as discussed in the preceding paragraph. This authority is available until September 30, 2026, or until the appropriations for credit subsidy supporting it are expended.
  - Title XVII Innovative Technology Loan Guarantee, Section 1706, authorized and appropriated funds to support guarantees of up to \$250 billion. Section 1706 should be used to help retool, repower, repurpose, or replace existing energy infrastructure that has ceased operations, or to enable operating energy infrastructure to avoid, reduce, utilize, or sequester air pollutants or anthropogenic emissions of greenhouse gases. This authority is available until September 30, 2026, or until the appropriations for credit subsidy supporting it are expended.
  - Advanced Technology Vehicles Manufacturing Direct Loan Program is estimated to support approximately \$40 billion of loans. These loans finance U.S. manufacturing of fuel-efficient, advanced technology vehicles and qualifying components. Although the legislation does not provide a “cap” for this loan authority, the Loan Programs Office (LPO) estimates that appropriations for credit subsidy may support an estimated \$40 billion.<sup>5</sup> This authority is available through September 30, 2028, or until appropriations for credit subsidy costs supporting it are expended.
  - Tribal Energy Loan Guarantee Program (TELGP). IRA changed and increased this \$20 billion program. These loans can finance a broad range of energy development projects owned by Tribal Nations. The math for this authority contains two parts: (1) \$18 billion in new IRA expanded TELGP authority, (2) plus IRA created new rules and applicability for an existing \$2 billion TELGP authority that was authorized in the FY 2017 Consolidated Appropriations Act (Public Law 115-31) in such manner as to subsume the prior \$2 billion authority and to combine it with the new \$18 billion IRA authority, resulting in \$20 billion. This authority is available until expended.
  
- The IJA authorized and appropriated funds for the Carbon Dioxide Transportation Infrastructure Finance and Innovation Program loan guarantee program by an estimated \$20 billion. The LPO will manage this Program in partnership with the Department’s Office of Fossil Energy and Carbon Management. The loans are designed to support large capacity, common carrier carbon dioxide transport projects. The legislation does not include a ceiling for the maximum amount of loans that can be made for this authority; however, the LPO estimates that appropriations for credit subsidy and administrative costs may support an estimated \$20 billion.<sup>6</sup> This authority is available until expended.

---

<sup>5</sup> The LPO Annual Portfolio Status Report (Page 4): <https://www.energy.gov>

<sup>6</sup> The LPO Annual Portfolio Status Report (Page 5): <https://www.energy.gov>

The preceding information is summarized in the following table:

Law	Amount	Program	Purpose	Expiration	Statutory or estimated
<b>2023 Consolidated Appropriations Act</b> \$15 billion	\$15 billion	<b>Section 1703. Title XVII Innovative Loan Technology Guarantee</b>	Eligible projects must (1) avoid, reduce, or sequester air pollutants or anthropogenic greenhouse gas emissions, and (2) employ new or significantly improved technologies	Available until credit subsidy appropriation is expended	Statutory ceiling
<b>Inflation Reduction Act</b> \$350 billion	\$40 billion	<b>Section 1703. Title XVII Innovative Loan Technology Guarantee</b>	Identical to 2023 Consolidated Appropriations authority described above	Sept. 30, 2026	Statutory ceiling
	\$250 billion	<b>Section 1706. Title XVII Energy Infrastructure Reinvestment Program / Innovative Technology Loan Guarantee</b>	Retool, repower, replace, or repurpose existing energy infrastructure that ceased operations, or to enable energy infrastructure to avoid, reduce, utilize, or sequester air pollutants or anthropogenic emissions of greenhouse gases	Sept. 30, 2026	Statutory ceiling
	\$40 billion	<b>Advanced Technology Vehicles Manufacturing Direct Loan Program</b>	Finance U.S. manufacturing of fuel-efficient, advanced technology vehicles and qualifying components	Sept. 30, 2028	IRA removed a \$25 billion cap. \$40 billion is current estimated amount that may be supported by the credit subsidy appropriation
	\$20 billion	<b>Tribal Energy Loan Guarantee Program</b>	These loans can finance a broad range of energy development projects owned by Tribal Nations	Available until expended	Statutory ceiling
<b>Infrastructure Investment and Jobs Act</b> \$20 billion	\$20 billion	<b>Carbon Dioxide Transportation Infrastructure Finance and Innovation Program Loan Guarantee Program</b>	The loans are designed to support large capacity, common carrier carbon dioxide transport projects	Available until expended	Estimated amount based on the loan dollars supported by the credit subsidy appropriation

### Recent Legislation Expanded Department’s Grant Programs

Of the \$99 billion in supplemental appropriations to the Department, we estimate that \$65 billion will be distributed in grants and other financial assistance awards,<sup>7</sup> including the creation of 72 new programs. Beginning with the most recent legislation:

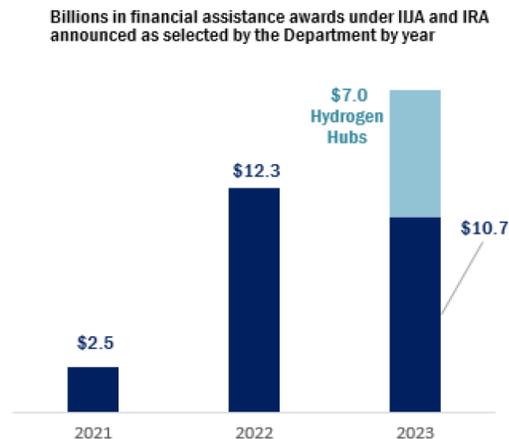
- The 2023 Consolidated Appropriations Act<sup>8</sup>—Congress added \$1 billion to the Department’s appropriations to provide grants to the Puerto Rico Energy Resilience Fund to build energy system resilience to major natural disasters. This is a new grant program.

<sup>7</sup> In this context, “grants” include all types of Financial Assistance programs, including grants, cooperative agreements, direct subsidies, prizes, and other non-contractual transactions. It is important to note that this number is not settled since awards are still being made, and the Department has some flexibility in the manner that the program funds are disbursed.

<sup>8</sup> Public Law 117-328

- IRA<sup>9</sup>—Of the \$35 billion in appropriations, we estimate that \$16 billion is slated for grants. The legislation funds 21 programs,<sup>10</sup> 15 of which are new programs.<sup>11</sup>
- IIJA<sup>12</sup>—Of the \$62 billion, we estimate that \$48 billion is slated for grants. The legislation funds 69 programs,<sup>13</sup> 56 of which are new programs.

The Department is already moving these funds. The Department reports that more than \$32 billion in awards have been selected, increasing rapidly over time, as shown in this chart. The volume and pace of these awards will increase significantly from FY 2024 through FY 2025. By way of comparison with historical awards volumes, in FY 2021, the Department awarded \$3.9 billion in financial assistance awards for enduring mission grants, not including the IIJA funds.



### Due Diligence Challenges Facing Both Loan and Grants Programs

History teaches us that certain factors make applied due diligence less rigorous, even when due diligence procedures may seem well drafted.

**Fast moving funds incentivize cutting corners in due diligence.** One category of loan guarantees worth an estimated \$250 billion expires on September 30, 2026—3 years from now. Another category of loan guarantees worth an estimated \$40 billion expires on the same date—\$290 billion over the next 3 years or, put another way, roughly \$8 billion per month over the next 36 months. There is no precedent for this level and pace of financing. In the interest of moving these funds out, on schedule, the Department may be incentivized to cut corners and skip rigorous due diligence steps that are needed to properly manage the risk of default.

Similarly, for grant programs, Department officials are under pressure to award grants and thereby move the clean climate program forward as quickly as possible. This goal directed pressure may also lead to cutting corners in due diligence procedures.

**There is a real risk that awards will be made to ineligible recipients.** For the innovative technology loan guarantee program, the loan applicant must demonstrate innovation

<sup>9</sup> Public Law 117-169

<sup>10</sup> <https://www.energy.gov/infrastructure/clean-energy-infrastructure-programs-department-energy>

<sup>11</sup> One of the new programs is Department Oversight for \$20 million, which captures funding for the OIG.

<sup>12</sup> Public Law 117-58

<sup>13</sup> <https://www.energy.gov/infrastructure/clean-energy-infrastructure-programs-department-energy>

in the technology being financed in the project. There is a real risk that “innovation” claims will be exaggerated by the applicant, or that baseless or marginally innovative proposals may be awarded financing. Compounding this risk is the pressure on the Department to make loans before authority expires. Should this occur, there is less money available for truly innovative technology projects.

Similarly, in the grants program, due diligence is crucial to ensure that awardees satisfy program participation criteria. The same incentives exist for grant applicants to cheat on eligibility and for Federal officials to approve the applications with too little verification.

**Due diligence is essential to prevent awards to foreign entities.** Both IJA and IRA include requirements that call for both loan and grant awards to be made to entities that advance the agenda of domestic technology development and jobs creation, and that seek to prevent awards to foreign entities. To help manage this risk, in March of this year, the Department set up a pilot “vetting” process through the “Research, Technology, and Economic Security Vetting Center.” This office intends to screen loan and grant awards for foreign influence, ownership, and control. However, this pilot process is new, still under development, untested, and will be called upon to screen numerous projects on a truncated timeline. This office is currently staffed by only three people. All these factors increase the risk that awards will be made to entities with foreign entanglements that go undetected.

Yet, award determinations were already underway, well ahead of the vetting center pilot. One of these projects raises the issue of balancing competing goals. Kore Power, an Idaho-based company that currently makes lithium-ion battery cells in China with Chinese technology and intellectual property, won a conditional commitment from the LPO in June 2023 for an \$850 million loan to help build its first major U.S. manufacturing facility in Arizona. In this case, the Department is moving the project forward on the grounds that U.S. jobs will be created deploying Chinese technology in the U.S., and with the belief that U.S. technology will not go overseas. While it appears that this financing project may support Congress’ goals of U.S. job creation, it clearly does not support the legislation’s goals of U.S. technology development since this project deploys Chinese intellectual property.

The OIG has conducted a number of investigations related to the theft of intellectual property and violations of grant terms and conditions. In fact, 35 percent of the grant fraud cases currently open are related to research security with a real risk that this research will go overseas. For example, a recent investigation conducted jointly by my office and the National Science Foundation OIG found that a principal investigator at the University of Kansas created a scheme to defraud the Government by failing to disclose on grant proposals to the Department an existing affiliation with, and contractual obligations to, a Chinese university. The grant recipient also failed to disclose this conflict of interest to the University of Kansas.<sup>14</sup>

There is every reason to conclude that foreign actors will seek IJA and IRA funds to advance development of clean energy technology, and that the Department’s due diligence procedures may not be sufficient to deal with this reality.

---

<sup>14</sup> <https://www.justice.gov/opa/pr/jury-convicts-university-kansas-researcher-hiding-ties-chinese-government>

**Due diligence needed to prevent “double dipping.”** Since 2009, there has been a broad prohibition against “double dipping”—the notion that an entity that was funded through one sort of Federal funding, such as a grant, would then use those Federal grant funds to apply for more Federal monies such as a loan. This risk is accentuated with the loan applicants and grant applicants competing for funding to develop innovative clean energy technologies. In other words, projects deemed worthy of grants may be considered as good candidates for the loans as well, but need to be carefully screened to ensure that double dipping is not occurring.

### **Additional Risks - Loan Program**

**What rate of loan default is acceptable?** The LPO faces enormous challenges. First, these loans are designed to create partial or total financing for projects that are otherwise too risky for commercial banks or private equity to accept. Stated differently, these projects would fail commercial due diligence. This raises the most fundamental question: What amount of risk is acceptable? This question should be discussed; acceptable risk should be defined; overall success for the program should also be defined; and the results should be tracked and reported.

In a commercial setting, default on the loan is what defines failure. If the lender is paid on the loan, the lender has been successful. Here, the LPO will be financing projects in full anticipation of some amount of default. What amount of default of these \$385 billion is acceptable?

**Indian Energy Loan Guarantee Program no longer requires “skin in the game.”** We note that IRA loosened controls that came with this program’s 2017 authority in two fundamental ways. First, the 2017 authority was for a partial loan guarantee, not to exceed 90 percent. Put another way, the loan applicant had 10 percent “skin in the game.” No deals were closed under these standards. IRA removed the 90 percent partial loan guarantee requirement and now allows for 100 percent financing of project costs. Second, IRA now guarantees loans from, and allows access to, the U.S. Treasury’s Federal Financing Bank loans, which reduces both fees and interest expenses. Together, these changes are certain to increase participation in the program and the risk of default. With increased risk should come increased due diligence procedures to add assurance that the taxpayer is being protected in this increasingly risky program.

### **Additional Risks - Grants**

**New programs are pushing out billions in grant money through newly designed processes using untested internal controls.** Overwhelmingly, the 72 new programs are for grants and financial assistance awards, awarding an estimated \$65 billion in appropriations. These new Federal programs raise immediate concerns such as acquiring and training expert staff and quickly developing effective internal controls. For these new programs in particular, there is a critical need for external oversight of these new Federal programs to help prevent foreseeable problems as early as possible.

**The Department has not taken concrete steps to ensure that sufficient resources are reserved to perform proper oversight over significant increases in grants to states, local government, and tribes.** As this money is awarded to these entities, it is then further dispersed to subrecipients. It is not yet clear whether the states, local governments, or tribes are equipped with sufficient staffing, or have adequate internal control systems in place, to protect these funds. Our early indicators are that states’ oversight resources are stretched and strained due to multiple competing priorities, including ongoing pandemic oversight commitments. Importantly, the passing of these Federal funds to others neither removes the Federal nature of the expenditure nor excuses Federal oversight, but it certainly increases risk. My office has been notifying Department leadership of these concerns for more than a year.

**The Department is planning to disburse billions of dollars using award vehicles it has little or no experience with.** The Department has some experience in administering financial assistance programs in the form of grants and cooperative agreements. However, the IIJA mandates programs that do not fit neatly into these categories. Some examples of these include direct subsidies for the \$6 billion Civil Nuclear Credit Program, competitive “prize” programs, and others. Accordingly, the Department established a Working Group on Innovative Funding Mechanisms to develop processes, policies, and procedures to use Partnership Intermediary Agreements<sup>15</sup> and “Other Transaction Authority” to make these atypical awards. We note that there are real risks associated with developing new processes to pay billions of dollars using award instruments for which the Department has little or no experience.

**Modern data analytics tools are not being used to prevent improper payment or to detect fraud, waste, and abuse in grant programs.** Historically, the Department has not gathered or required data from its many grantees in sufficient detail to support modern data analytics capabilities, prevent and detect improper payments, or detect fraud. Other Federal agencies have learned a great deal about the power afforded by data analytics capabilities applied to high volume transactions. In late July 2023, the Department issued program requirements and grant application instructions that appear to miss an opportunity to require the type of data that has served other agencies so well during the pandemic. The OIG is currently evaluating opportunities for the Department to require additional data to be gathered by grantees for rebate program beneficiaries, in a secure manner, that can be used to prevent improper payments and to detect fraudulent patterns and actions. Additionally, the OIG team is exploring questions related to information sharing opportunities and other tools such as using the U.S. Treasury’s “Do Not Pay” tool. This work is already well underway. The OIG report will identify additional opportunities for the Department to use on other grant programs to modernize data analytics capabilities.

**The Department has a poor track record auditing grantees.** Federal regulations require that recipients spending more than \$750,000 in Federal funds must undergo an annual audit by an independent auditor. Commonly called “Single Audits” these audits are designed to help ensure that recipients have adequate accounting systems and effective internal controls. It is critical that these independent audits are conducted. It is also critical that the granting agency monitor compliance and follow up on the issues identified by these and other audits. This

---

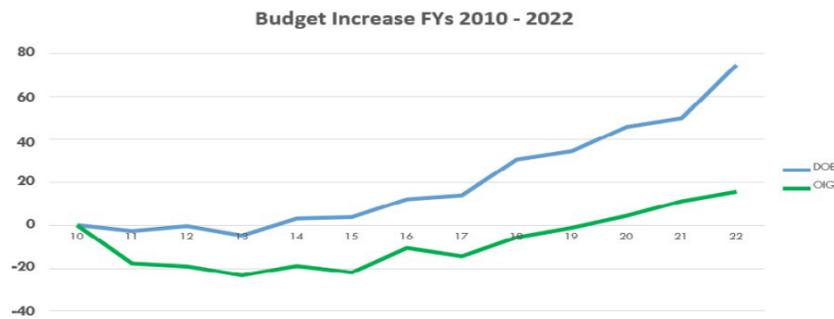
<sup>15</sup> 15 U.S.C. § 3715, Use of Partnership Intermediaries

oversight framework is only effective if it is implemented and overseen appropriately by granting agencies.

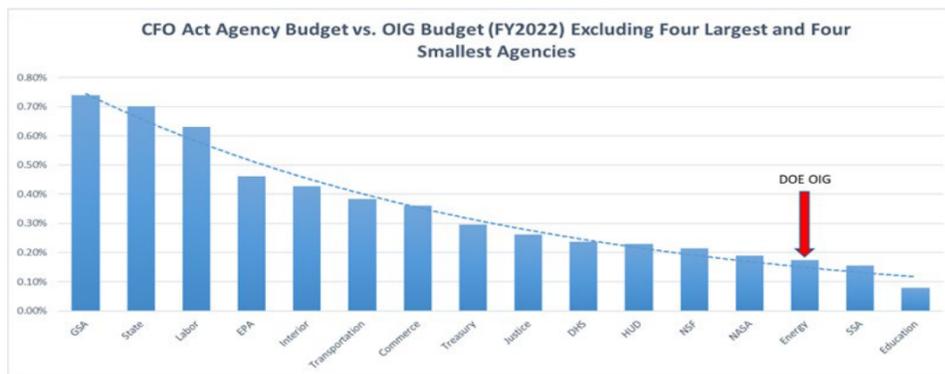
The OIG has identified areas where the Department could improve its oversight in this area. For example, a March 13, 2023, Department OIG audit found that the Department’s Office of Science failed to ensure that required annual audits of for-profit recipients of Small Business Innovation Research grants had been completed. Award expenditures totaling \$56,835,650 that were not audited, as required, exposed the Department to an increased risk of fraud, waste, and abuse.

### Underfunded OIG Oversight

**Lack of adequate base funding for the OIG.** Prior to the passing of the three pieces of supplemental legislation discussed above, the OIG was already significantly underfunded. The following chart demonstrates the long-term and growing gap of OIG funding growth compared with the growth of the Department’s budget prior to the more recent legislation:



The next chart provides a glance of Inspector General discretionary funding for many Chief Financial Officers Act agencies, as of FY 2022:



**Supplemental legislation underfunded the OIG.** To further exacerbate the historic underfunding issue, the OIG received only \$62 million, or 0.10 percent of the funding provided

to the Department over a 5-year period under IJA, to provide oversight of these new infrastructure projects. When compared with other OIGs that received money under IJA, we were again substantially underfunded as shown in the following table:

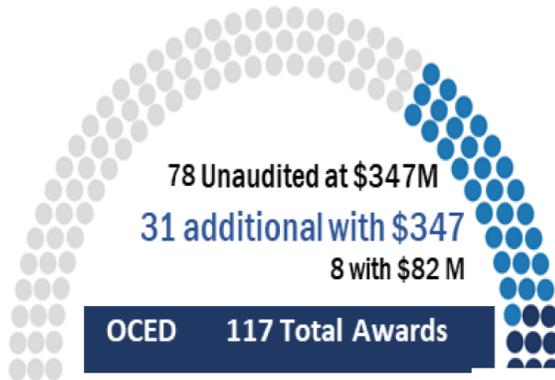
	IJA Agency Funding	IJA OIG Funding	OIG Percent of Agency Funding
EPA	\$61 billion	\$269 million	0.44%
HHS	\$4 billion	\$17 million	0.44%
DOI	\$28 billion	\$99 million	0.35%
USDA	\$8 billion	\$27 million	0.34%
DHS	\$8 billion	\$20 million	0.25%
DOE	\$64 billion <sup>1</sup>	\$62 million	0.10%

Also, IRA appropriated only \$20 million to the OIG, or 0.05 percent of the funding provided to the Department, to oversee those programs. Notably, there was no provision for additional OIG funding in the expanded programs in the FY 2023 appropriations to include an expansion of \$15 billion in loan program authority and a new \$1 billion in appropriations for the Puerto Rico Energy Resilience Fund. Notice the pattern: The OIG has increasing oversight mandates for supplemental programs while getting reduced resources for oversight.

An appropriate starting point for proper funding for the OIG is at 0.35 percent of the Department’s budget. We arrived at this conclusion by examining FY 2022 funding levels for the OIGs of the Chief Financial Officers Act agencies, as well as the more current funding of the OIGs impacted by IJA and IRA. The 0.35 percent falls into the mid-range. Given the significant risks for the Department, this percentage may be too low. However, it is a starting point and much needed.

**Needed oversight work is not being performed, and cannot be performed, without significant increases in funding.** It is crucial for policymakers in Congress and Department leadership to understand how the current underfunding of OIG programs constrains the OIG’s oversight plans. Our oversight plan for audits and inspections is organized into two categories – Federal- level programs and award level projects. First, it is imperative that the Department’s 72 new programs receive independent oversight. If properly funded, the OIG’s oversight plans would include about 80 audits and inspections for the **Federal- level programs**, including most of the 72 new programs. Currently, the OIG is only funded to perform about 20 reviews of Federal-level programs over a very long-time horizon. Regarding the second category, the OIG’s audits and inspections at the **award-level**, the OIG is currently only able to plan for about 50 award-level oversight projects—less than 1 percent of the anticipated more than 5,000 awards. The OIG should be planning more than 400 projects at the award level. This level of oversight is both inadequate and irresponsible.

The following charts show what impact the OIG’s budget shortfall has on our oversight responsibilities. Specifically, the Department’s Office of Clean Energy Demonstrations is the largest new program with about \$25.7 billion in appropriations that anticipates making about 117 total awards. However, the OIG can fund only 8 award-level audits at current funding levels (dark blue) compared with the 31 additional (39 total) award-level projects we conclude that we should do (light blue) given the massive amount of risk.



Similarly, for the Department’s State and Community Energy Program, a \$15.3 billion program that anticipates making about 3,700 awards, the OIG can only fund 15 award level projects at current funding levels (dark blue) whereas risk factors indicate we should perform 94 more (light blue) award-level reviews (total of 109). These are just two examples from our oversight plans.



**How much is the OIG funding shortfall?** The President’s FY 2024 Budget includes \$165.2 million for the Department OIG to be used until expended. If the President’s Budget is enacted as is, it would leave a remaining shortfall of \$16.8 million in our base budget. However, the current version of the Senate Energy and Water Development Fiscal Year 2024 Appropriations Bill provides only \$86 million to the OIG, leaving a base budget shortfall of \$96 million.

Additionally, the OIG has a shortfall of \$264.7 million to oversee IIJA, IRA, and the Puerto Rico Energy Resilience Fund. The following chart shows the OIG’s funding shortfall to conduct proper oversight of the three pieces of recent supplemental legislation:

**Supplemental Shortfall -- Exclusive of the Loan Portfolio**

Bills	DOE	OIG	Current Percent OIG to DOE	OIG Estimated Requirements	OIG Estimated Funding Shortfall
IIJA	\$62.5 B	\$62.5 M	0.10%	\$218.6 M	\$156.2 M
IRA	\$35.0 B	\$20.0 M	0.06%	\$125.0 M	\$105.0 M
PR-ERF	\$1.0 B	\$0.0 M	0.00%	\$3.5 M	\$3.5 M
<b>Total</b>	<b>\$98.5 B</b>	<b>\$82.5 M</b>	<b>0.08%</b>	<b>\$347.1 M</b>	<b>\$264.7 M</b>

**The Department is apparently seeking to enhance its own oversight resources using the same type of transfer mechanism.** The statutory 3 percent funding cap for Program Direction placed on the Department under IIJA limits the Department’s ability to conduct effective oversight. This funding cap applies to the following programs: Energy Efficiency and Renewable Energy; Cybersecurity, Energy Security, and Emergency Response; Electricity; Fossil Energy and Carbon Management; and the Office of Clean Energy Demonstrations. The Department is apparently seeking to correct this. The FY 2024 Senate Bill contains language increasing the 3 percent cap on “Program Direction” to 5 percent. The OIG supports the Department receiving additional funds for conducting its own oversight.

The FY 2024 House Bill provides a transfer of funds from the Department’s unobligated balances under both IIJA and IRA to the OIG; however, the transfer falls short of the 0.35% necessary, and does not provide for a transfer of funds from the Puerto Rico Energy Resilience Fund. Our requested transfers would provide the OIG with the \$264.7 million shortfall by transferring funds from the Department’s unobligated balances under IIJA, IRA, and the Puerto Rico Energy Resilience Fund. Therefore, the transfers do not require any new appropriations. These transfers are critical for ensuring that the funding provided to the Department under these pieces of legislation are used for their intended purposes.

**The OIG has important work underway and planned.** Although the OIG remains significantly underfunded, we have engaged in a great deal of work to help prevent fraud, waste, and abuse in the Department’s expanded loan and grants programs. Since the passage of IIJA, the OIG has conducted 227 Fraud Awareness Briefings that reached more than 9,160 Federal employees, contractors, grantees, external auditors, law enforcement, as well as state, local government, and tribal representatives. We have also worked closely with other OIGs who have received funding under these pieces of legislation to identify risks and best practices. I am

currently serving as the co-chair of the Council of the Inspectors General on Integrity and Efficiency's IJA Working Group.

Since early 2022, my office has held dozens of meetings with senior Department leadership to pose questions to them regarding risks faced by the new programs and to identify issues the OIG has reported during the performance of prior work. In this way, we have safeguarded our independence while helping the Department identify risks. Additionally, between April 2022 and August 2022, the OIG issued four capstone reports summarizing previous work. These reports targeted specific programmatic areas that will receive substantial funding under the new legislation. These reports discuss the loan program;<sup>16</sup> the Weatherization Assistance Program;<sup>17</sup> financial assistance awards;<sup>18</sup> and Clean Energy Demonstration Projects.<sup>19</sup> Issues reported in these reports include recipient fraud; insufficient Federal staffing; inadequate oversight of projects; circumvention of project controls; inadequate internal controls; and lack of recipient-level controls.

Also, my office has oversight projects underway addressing fraud risk in Home Energy Rebate Program grants; an audit of the Weatherization Assistance Program; adoption and use of data analytics capabilities; and an inspection of the Puerto Rico Energy Resilience Project. We are about to begin working on conflict-of-interest issues in the LPO.

Further, given the importance of the risks posed by foreign actors to Department intellectual property and national security, our Office of Inspections, Intelligence Oversight, and Special Projects has recently begun an inspection focusing on the Department's compliance with requirements of Department of Energy Order 486.1A, *Foreign Government Sponsored or Affiliated Activities*. The Order prohibits Department employees and contractors from participating in foreign government-sponsored talent recruitment programs and also restricts participation in other foreign government-sponsored or affiliated activities of a "foreign country of risk." Additionally, we are planning a joint project with the OIG of the Intelligence Community in FY 2024 to evaluate Department security processes in accordance with the requirements in Security Executive Agent Directives and Department Orders.

### Closing Remarks

I would like to recognize the key role that bipartisan efforts from Congressional oversight committees have played over the years in advancing Government transparency and program integrity. We are all aware of the important work that Congressional committees have done with Inspectors General over the years. Thank you for your continued support of the independent oversight work performed by my office and the Inspector General community. We look forward to continuing to work on behalf of the taxpayers to ensure that Federal infrastructure and energy programs are operating effectively and efficiently, and to prevent and detect fraud, waste, and abuse. I appreciate the opportunity to testify here today, and I look forward to answering your questions.

---

<sup>16</sup> <https://www.energy.gov/ig/articles/special-report-doe-oig-22-34>

<sup>17</sup> <https://www.energy.gov/ig/articles/special-report-doe-oig-22-30>

<sup>18</sup> <https://www.energy.gov/ig/articles/special-report-doe-oig-22-40>

<sup>19</sup> <https://www.energy.gov/ig/articles/special-report-doe-oig-22-39>

## **FEEDBACK**

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We aim to make our reports as responsive as possible and ask you to consider sharing your thoughts with us.

Please send your comments, suggestions, and feedback to [OIG.Reports@hq.doe.gov](mailto:OIG.Reports@hq.doe.gov) and include your name, contact information, and the report number. You may also mail comments to us:

Office of Inspector General (IG-12)  
Department of Energy  
Washington, DC 20585

If you want to discuss this report or your comments with a member of the Office of Inspector General staff, please contact our office at 202–586–1818. For media-related inquiries, please call 202–586–7406.