OFFICE OF INSPECTOR GENERAL

U.S. Department of Energy

Management Challenges at the Department of Energy — Fiscal Year 2025

DOE-OIG-25-05

November 2024

Department of Energy
Washington, DC 20585

November 20, 2024

MEMORANDUM FOR THE SECRETARY OF ENERGY

SUBJECT: Special Report: *Management Challenges at the Department of Energy — Fiscal Year 2025*

As the top management challenge, the Office of Inspector General (OIG) continues to highlight the significant risks posed by the Infrastructure Investment and Jobs Act, Inflation Reduction Act, and the Puerto Rico Energy Resilience Fund.

In part because of these risks, the OIG identified approximately $1 billion in potential savings and recoveries at the Department of Energy in fiscal year 2024. Notably, because only about 4 percent of the OIG's recommendations were readily monetized, the value the OIG provided to the Department far exceeded that $1 billion.

The OIG's work could not have been successful without your cooperation. Thank you for cooperating with the OIG during your tenure at the Department. The tone at the top certainly matters.

As you prepare to leave the Department, I hope you will support the OIG's pending budget request. Preventing fraud, waste, and abuse in connection with the Infrastructure Investment and Jobs Act, Inflation Reduction Act, and the Puerto Rico Energy Resilience Fund will be extremely difficult absent additional funding.

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

UNPRECEDENTED CHALLENGES UNDER RECENT LEGISLATION

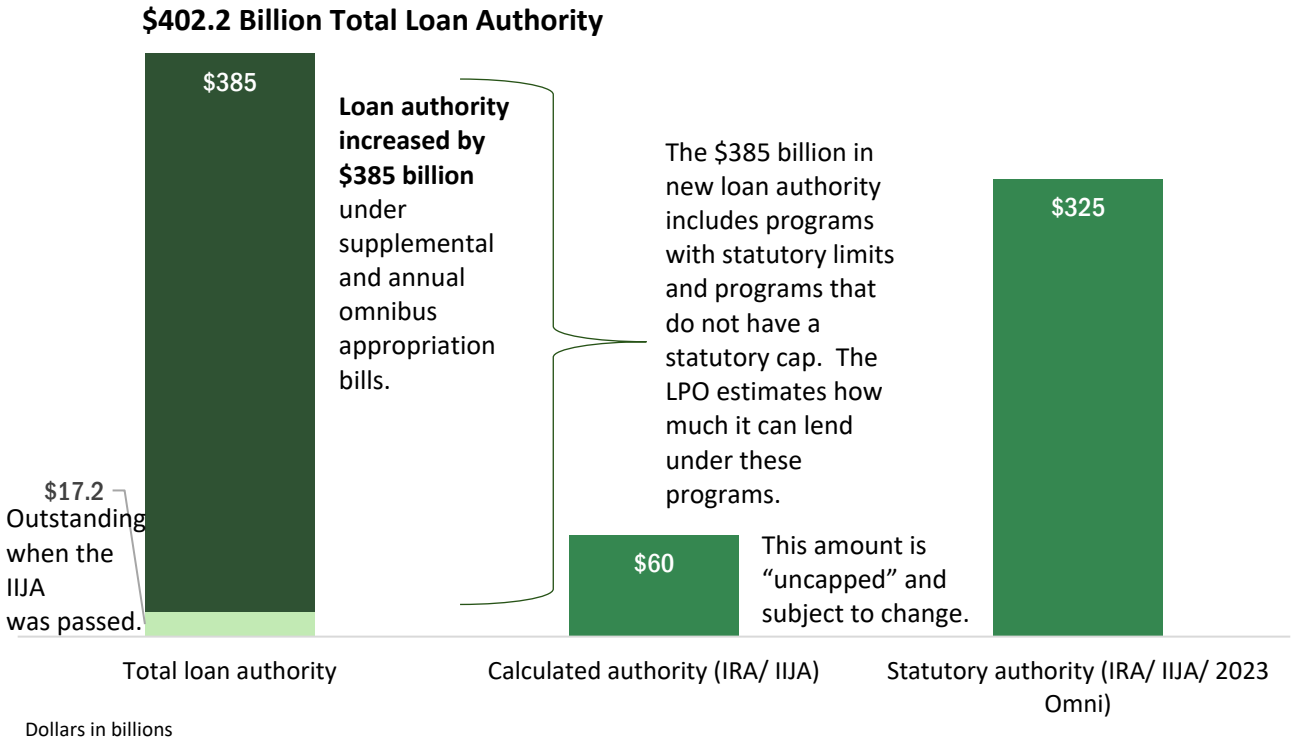
Overseeing the Department of Energy's High-Risk Portfolio Under the Infrastructure and Investment Jobs Act, CHIPS and Science Act, Inflation Reduction Act, and Puerto Rico Energy Resilience Fund

There is tremendous risk to the taxpayer from the recent historic expansions of Department of Energy programs. Passage of the Infrastructure Investment and Jobs Act (IIJA) in November 2021, both the CHIPS and Science Act (CHIPS Act) and Inflation Reduction Act (IRA) in August 2022, and the Puerto Rico Energy Resilience Fund in December 2022 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.

Special Focus on Loan Programs Office Risks

The Office of Inspector General (OIG) is particularly concerned about the risks associated with the rapid expansion of the Loan Programs Office (LPO). When the IIJA—the first of the massive supplemental appropriation bills—was signed into law, the LPO had $17.2 billion of outstanding loans. From 2021 through 2023, the IIJA, IRA, and 2023 Omnibus Appropriations Law increased the LPO's lending authority by at least $385 billion to a total of at least $402.2 billion.[1] This almost half a trillion in authority is more than 23 times that of the LPO portfolio balance as of November 2021, when the IIJA was signed. To illustrate:

[1] The OIG had been tracking an estimated $385 billion in expanded loan portfolio enabled by the IIJA and IRA, as managed by the LPO program. Of this amount, $60 billion is an estimate, as the statute has no cap/unrestricted cap for those programs. LPO will make loans until the credit subsidy supporting the loans are committed. Estimates for these programs will change annually. Additionally, the $385 billion estimate does not account for an additional loan portfolio that the Grid Deployment Office is now standing up, which includes more than $2 billion of credit subsidy, which may support an additional large portfolio of loan guarantees for electrical transmission lines. The Department does not have an official estimate for what size portfolio this appropriation can support, but it may be between $20 to $40 billion. It is important to understand that the LPO estimated portfolio of loans and guarantees will likely increase.

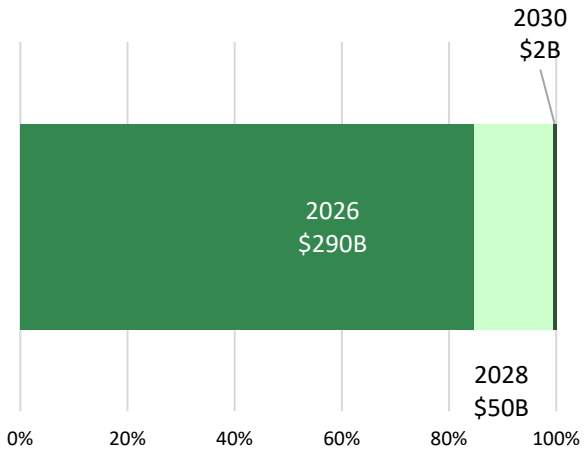


Increase in the LPO's Loan Authority

The OIG has identified, at a minimum, the following risks posed by this loan authority:

1) Near-term deadlines could create pressure to cut corners.

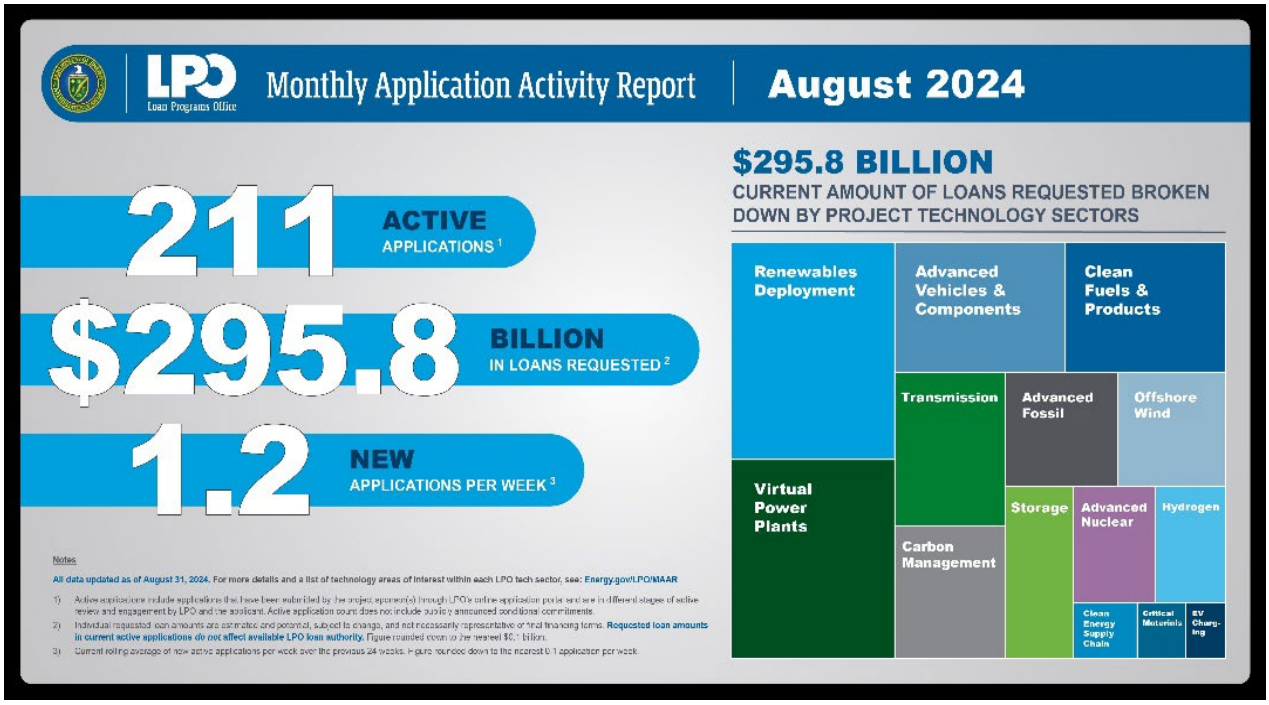
Most of the loan authority will expire from 2026 through 2030, meaning the LPO must build its portfolio with deals collectively worth hundreds of billions of dollars on accelerated timeframes. As shown in the figure to the right, $290 billion of expanded loan authority will expire September 30, 2026, just 2 years from now. An additional $50 billion and $2 billion in authority will expire, respectively, at the end of fiscal year (FY) 2028 and FY 2030.



The pressure to beat these deadlines introduces the risk that the LPO will enter into loans it otherwise would not, absent the looming deadlines, because of insufficient time to conduct

rigorous due diligence, to negotiate terms that could effectively mitigate the risks identified during the due diligence, and to consider alternative projects that might offer a more favorable risk profile.

Applications are being submitted to the LPO rapidly. Specifically, the LPO reported 211 loan applications worth $296 billion in August 2024. This is an average of about $1.4 billion per loan application, with new loan applications coming in regularly. This volume of applications, looming deadlines to enter into inherently risky deals, and the hundreds of billions of dollars at stake make this one of the most urgent and significant management challenges facing the Department today.



2) Innovative projects, not likely to otherwise be funded by the private sector, come with inherent risks.

Fundamentally, the purpose of the Department's loan programs is to provide financing for projects that, without the LPO backing, could not be obtained from the commercial banking or private equity sectors. This fundamental risk warrants more rigorous due diligence procedures, where those reviewing the loan applications should be afforded more time rather than less.

3) Accelerated due diligence may fail.

The LPO's due diligence process is the Department's principal internal control process to ensure that the loan applications are sufficient to satisfy three overarching goals. First, the loan application must meet Federal requirements for the loan program. Each of the loan programs have requirements that leave plenty to interpretation, which introduces risk into the system that loans may be awarded for purposes other than those intended by Congress. Second, the due diligence process must assess whether the project is technically feasible and commercially

scalable, which may prove challenging for some of the loan applicants that must scale unproven technologies. Third, the due diligence process must ascertain the financial viability of the proposal over the loan's entire term. This is particularly challenging for new markets, rapidly changing technologies, and newly created companies.

4) The Department may fund foreign adversaries.

Congress clearly intends for public financing to benefit domestic industry, create domestic jobs, and reduce vulnerabilities created by over-dependence on suppliers with foreign ties and the risk of foreign exploitation of domestic research efforts. Congress did not intend to benefit our foreign adversaries. Avoiding such benefits, however, will require careful vetting of grant and loan applicants for foreign adversary entanglements, which is something not historically done by the Department. On March 1, 2023, the Department did direct that the Research, Technology, and Economic Security Vetting Center (Vetting Center) be established for this purpose, to identify foreign adversary entanglements. This Vetting Center, however, is new, evolving, and has already failed to prevent applicants with such prohibited foreign adversary connections from being approved.

Even beyond domestic supply chain issues, the Vetting Center must also operate to prohibit a broad range of Federal loan and grant funds from ending up in the control of our foreign adversaries.

For example, the OIG has already identified two instances in which the Department announced grants to entities with suspected ties to foreign entities of concern. The OIG presented this information to Department officials, who then appropriately cancelled both awards. These two awards alone were worth a combined total of about $400 million.

5) These risks compound to create an outsized risk of default.

All of these risks compound one another in a manner that, ultimately, creates a heightened risk of loan default with the taxpayer picking up the bill. With more than $400 billion of possible loans and guarantees, this is one of the largest financial risks facing the Department today.

Risks Associated With the New Financial Assistance Programs

With the funding received under recent legislation, the Department stood up 72 new programs—such as an $8 billion Regional Clean Hydrogen Hub Program and a $6 billion program for battery material processing, manufacturing, and recycling—and significantly expanded other programs, such as the Weatherization Assistance Program, which went from receiving $313 million in appropriations in FY 2022 to receiving $3.5 billion under the IIJA.

Of the $99 billion in appropriations contained in the IIJA and IRA, the Department has published more than $67 billion in funding announcements and, of that, has announced more than $50 billion in awards—largely for grants, cooperative agreements, and other financial assistance awards.

The Department must prevent the theft and waste of these funds rather than follow the "pay and chase" model, in which money goes out the door with few controls, and agencies must later expend considerable resources to recover a mere portion of fraudulently spent and misspent money. Effective "front end" oversight can avoid billions of dollars in losses.

The OIG's oversight work continues to raise red flags about the Department's ability to avoid making awards and approving transactions that pose risks to Department programs. Inspector General Donaldson testified before Congress in April 2023 and again in October 2023 about concerns such as newly designed and untested internal controls, potential capacity challenges faced by grant recipients, and an unprecedented level and pace of loan financing, much of it to fund projects with supply chains historically dependent on foreign adversaries. These concerns persist.

The OIG has recently reported on the proper collection and use of applicant identification data, which is one proven internal control to prevent fraud. Such controls are especially important for programs relying on third parties to further distribute Federal funding. These programs are a high-value target for individuals and criminal groups to exploit. The Department's State and Community Energy Program's $4.3 billion Home Rebates Program is one such program. Under this program, the Department provides grants to states and U.S. territories, which then convey funds to applicants via rebates. We concluded that the data that the Department intends to collect and require States to collect from recipients leaves concerning gaps that will hinder both the Federal Government and the States' ability to prevent and detect fraud.

The OIG has planned an oversight campaign at the award level for these and other high-risk, high-dollar programs administered under the Department's new and expanded mission areas. OIG auditors and OIG-hired independent audit firms will conduct audits of both grantees and sub-grantees to test their eligibility for the funding awarded to them, whether the activities undertaken are allowed under the award, compliance with cost principles, and whether they are conducting adequate sub-recipient monitoring.

Conclusion

Department leadership, as stewards for these new and expanded programs, has a duty to ensure that tax dollars entrusted to it are used as intended by Congress. The OIG concluded that appropriately managing the combination of risks to the taxpayer that are present in the massive expansion of lending authorities, together with the historic expansion of financial assistance award programs, are the most significant management challenge facing Department leadership today.

MODERNIZING OVERSIGHT AND MANAGEMENT

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

"The U.S. energy sector is a target for cyber criminals and for foreign adversaries, alike."

– Anne Neuberger, Deputy National Security Advisor to President Biden for Cyber and Emerging Technologies

Photo courtesy of Shutterstock, 2024

Significance of the Issue – Cybersecurity

Protecting and enhancing the security of the Department's information technology and operational technology assets, including critical infrastructure and high value assets, is crucial to fulfilling the Department's unique mission set spanning energy and nuclear security, grid modernization, scientific research and discovery, and cleaning up the environmental impacts caused by decades of nuclear weapons development and Government-sponsored nuclear energy research. The Department is also responsible for operating and securing critical infrastructure that supports the electric systems across 34 states and the operation of the Nation's Strategic Petroleum Reserve.

The Department possesses high-value assets that are so critical to the agency that the loss or corruption of the information or loss of access to the system would have a serious impact to the agency's ability to perform its mission or conduct business. The sensitivity of the information within these assets makes them ideal targets for criminal, politically motivated, or state-sponsored actors for either direct exploitation of the data or causing a loss in public confidence.

Similarly, the Department has a significant footprint of industrial control systems (ICS). The convergence of physical and cybersecurity processes and the increasing integration of ICS with business networks and internet-based applications has vastly increased the prevalence and complexity of cyber threats to ICS. This threat was highlighted recently by the Government Accountability Office's (GAO) report, *Nuclear Weapons Cybersecurity: Status of NNSA's Inventory and Risk Assessment Efforts for Certain Systems* (GAO-23-106309, June 2023), which identifies shortcomings with the identification, assessment, and mitigation of cyber risks to specific weapons or manufacturing equipment.

Cybersecurity is a critical aspect of the Department's overall security posture and one of the Department's highest risks. 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. Recent reports have highlighted the increase in attacks by state-sponsored adversaries on Federal agencies, military installations, and the Nation's critical infrastructure, which could lead to devastating consequences in the event of a cyber breach, including loss of life, property damage, and disruption of the essential services and critical functions upon which society relies.

Department Progress – Which Includes Issuing a Cybersecurity Strategy

The Department issued its Cybersecurity Strategy in January 2024, which aligns with the National Cybersecurity Strategy. The Department's strategy defines the integrated approach it will use to reduce cybersecurity risk given its diverse missions. The strategy was developed to achieve a safe, secure, and resilient cyber environment, which requires the Department to take a risk-based approach through cost-effective investments to reduce cyber risk. In April 2024, the Department also updated Department Order 205.1D, *Department of Energy Cybersecurity Program*, which now includes direction related to Zero Trust Architecture implementation, security and use requirements for cloud computing, and new guidance related to national security systems and portable electronic device security. In February 2024, the Department collaborated with the National Association of Regulatory Utility Commissioners to develop a set of cybersecurity baselines for electric distribution systems and the distributed energy resources that connect them.

The Department has also implemented various mechanisms to improve cybersecurity-related collaboration across the enterprise and with international partners. For example, the Office of the Chief Information Officer (OCIO), in collaboration with other Department programs, staged its Cybersecurity and Technology Innovation Conference that included topics such as operational technology risks, supply chain management, and the adoption of artificial intelligence (AI). Cybersecurity continues to be a point of emphasis discussed by various working groups, including the Information Management Governance Board, the Department Cyber and Information Technology/Operational Technology Executive Cyber, and IT Council. Further, 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.

These are important steps, but actual implementation of improved safeguards remains a significant challenge.

Challenges – Which Include Department Contractors Implementing and Assessing Their Cybersecurity Environments Against Outdated Requirements

Even with limited oversight, the OIG has identified numerous weaknesses in cybersecurity within the Department. These weaknesses, if exploited, could cause significant harm to the Department or the public.

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. In some cases, Department programs and sites report needing funding to close recommendations issued by the OIG. Some officials report being faced with difficult choices between addressing cybersecurity weaknesses or conducting mission-specific work, such as environmental clean-up, reducing the threat of nuclear proliferation, or conducting critical research at one of the many National Laboratories. This challenge was evident in our report, *The Department of Energy's Unclassified Cybersecurity Program - 2023*, which notes that the Department was unable to fully address 30 percent of the 73 recommendations made by the OIG in the prior year.

The Department also continues to encounter challenges implementing Federal mandates, addressing evolving threats, and mitigating shortages in the cyber workforce. Further, the Department's existing governance structure impacts its ability to respond to cybersecurity evolving risks and mandates. While the Department has an OCIO with broad responsibilities, the Department's decentralized organizational structure impedes the OCIO's ability to manage and combat cybersecurity risks facing the Department. The Department lacks a centralized organizational structure to oversee enterprise-level risks and to obtain, process, and correlate real-time cyber data. This impedes the OCIO's ability to manage security across the enterprise. The governance structure is exacerbated by a general lack of correlating authoritative data and using performance metrics to enhance cybersecurity oversight.

The Department continues to fall behind changing cybersecurity requirements and enhancements. Despite Department directives requiring implementation of the latest Federal cybersecurity guidance, 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. For example, the OIG's FY 2024 evaluation of the Department's unclassified cybersecurity program found that four of six sites reviewed had not fully implemented the requirements of the National Institute of Standards and Technology Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, issued more than 4 years ago. In fact, more than 80 percent of the 101 systems tested were still operating under outdated requirements. Contractors have reported that contractual requirements were not communicated to them or were not incorporated into their contracts timely. In many cases, officials indicated that while new requirements need to be implemented, they are underfunded or not funded at all. Officials have also expressed concerns that lines of authority are not clear. Some sites are taking cybersecurity direction from the site

offices overseeing them but not taking direction from the Department's OCIO. Some site officials have also resisted OCIO efforts as so-called "unfunded mandates" and continue to pursue locally focused solutions for problems that require 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. Given these challenges, the OIG has initiated a review to determine whether the Department implemented an effective governance process over information technology and cybersecurity management.

Furthermore, Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*, issued in May 2021, requires agencies to advance toward implementation of a Zero Trust Architecture to improve cybersecurity, visibility, and controls, among other things. The Office of Management and Budget also issued Memorandum 22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, which set the goal for agencies to meet specific cybersecurity standards and objectives of a Zero Trust Architecture by the end of FY 2024. The OIG's ongoing review of the Department's implementation of Zero Trust Architecture found that while the Department was making some progress, it was unable to fully meet the requirements of the memorandum.

EO 14028 also directed agencies to centralize and streamline access to cybersecurity data to drive data analytics for identifying and managing cybersecurity risks. However, the Department continues to be challenged with obtaining real-time, or even near real-time, authoritative data, including from its management and operating and prime contractors. This impacts its ability to detect and respond to threats in a timely manner across the entire enterprise. Instead of having real-time or near real-time data feeds from the various networks and systems supporting the Department's mission, it relies heavily on old school data calls—which are prone to delays, errors, and inconsistencies—to obtain information on the sites' security posture. As previously reported by the OIG, the Department could substantially benefit from leveraging sources of network information to conduct cyber analytics at the enterprise level to gain more visibility for making risk-based decisions. This would also enable the Department to use data analytics to help prioritize the use of limited resources.

Combating the Theft of National Security Information and Intellectual Property – Research Security

"While international cooperation is essential to accelerate research and development, some governments are aggressively pursuing access to U.S. science and technology advancements and intellectual property to the detriment of our economic prosperity and security."

– Department of Energy Office of Science

Photo courtesy of Shutterstock, 2024

Significance of the Issue – Theft by Foreign Adversaries

Safeguarding the Department of Energy's intellectual property and protecting national security information is of the utmost importance. Research security is necessary to protect the Department against the theft of valuable research and development to the detriment of national or economic security, and to protect our interests against foreign government interference.

Over 90 percent of the Department's more than $50 billion in annual funding is disseminated to contractors, which include the contractors running the National Laboratories, including the National Nuclear Security Administration (NNSA) research facilities. The Department and its contractors are responsible for complying with the requirements of National Security Presidential Memorandum 33, which requires that the Department maintain an effective research security program. Such a program must include a broad range of tools, including cybersecurity, physical security, protections against allowing spies and thieves within these facilities, and other matters. The relationship between the Department's facilities and academia makes research security particularly challenging.

The OIG is currently partnered with the Intelligence Community Inspector General to examine and evaluate a range of research security activities to counter foreign influence at select National Laboratories. This report is expected in summer 2025.

Research security concerns must also be carefully considered across Department programs to avoid giving Federal grant and loan funds to foreign adversaries, which could further empower those foreign adversaries. The Department should avoid granting or loaning funds under the IIJA and IRA to the same foreign adversaries that the Federal Bureau of Investigation has

identified as "the greatest long-term threat to our nation's ideas, innovation, and economic security."[2] If the Department is not careful, it could end up funding our foreign adversaries' activities – the same foreign adversaries that seek to illicitly acquire the research being developed in the Department's world class research facilities.

The Department's loan authority has increased to over $400 billion under the IIJA and IRA. It is critical that the Department ensure this unprecedented amount of money does not end up in the hands of our foreign adversaries.

According to the Congressional Research Service,[3] the Department budgeted $22.25 billion for *R&D and Related Activities*[4] in FY 2024. Most of this is spent by Department contractors at National Laboratories. Much of the remainder is awarded in the form of grants. In FY 2024, the Department awarded $10.9 billion[5] in grants, up from $9.12 billion in 2023. The OIG anticipates that the amount will continue to increase as additional grants are awarded under the IIJA, the CHIPS Act, and IRA. While some of this work is for fundamental research that is freely published in the public domain, much of it is subject to intellectual property protections, national and economic security considerations, and/or restrictions limiting the extent to which foreign firms could be involved such as advanced battery manufacturing, clean energy demonstration projects, and advanced/small modular nuclear reactors.

All of the Department's 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 steal information from the Department's funded research.

Department Progress – Which Includes Establishing the Vetting Center

Since our FY 2024 Management Challenges report, the Department has taken some steps to address this challenge. For example, the Department has reinvigorated its Office of Intelligence and Counterintelligence by changing its leadership and working to acquire additional funding.

In addition, on March 1, 2023, the Department directed that the Vetting Center be established to vet applicants for its vastly expanded grant and loan programs. The Department has made some progress beginning to staff and develop this organization. For example, on January 26, 2024, a memorandum was issued by the Deputy Secretary establishing a Vetting Center Policy Working Group and setting forth the Working Group's scope and function.

[2] Statement made by Christopher Wray, Director, Federal Bureau of Investigation, November 15, 2023, before the Committee on Homeland Security, United States House of Representatives.
[3] https://crsreports.congress.gov/product/pdf/R/R47564 (pp. 23, 24).
[4] Actual spending for *R&D and Related Activities* was not available at the time of this report.
[5] https://www.usaspending.gov/search/?hash=565ed2e3afa981ef643cf983ffa689bc.

Additionally, the OIG has seen progress within one Department program office, the Office of Energy Efficiency and Renewable Energy. This program office has demonstrated a commitment to preventing the theft of intellectual property by instituting prohibitions on affiliation with foreign talent programs from countries of concern for all prospective IIJA-funding recipients, and by signaling it will widen such restrictions to all financial assistance recipients for future funding opportunity announcements.

Challenges – Which Include Formalizing Conflict of Interest Language and Building a Robust Vetting Center

While the Department has made some effort to mitigate research security risks, much remains to be done in this area. As noted above, at least one program office has made progress in this area, but we have yet to see that these steps have been taken more broadly across the complex. It is critical for the Department to prioritize these efforts and ensure it has the adequate tools and resources to effectively prevent the theft of intellectual property and national security information consistently across all program offices. With the significant increase in funding allocated under the IIJA, the CHIPS Act, and IRA, it is increasingly important for the Department to coordinate the review of proposals with all available resources, such as the Vetting Center, to effectively minimize the risk to national security, and the risk of theft of intellectual property.

The Department must also provide sufficient resources to the Vetting Center so that it can fulfill 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. The Department must also design and implement enforcement tools to deter and take action against individuals who have stolen valuable U.S.-owned intellectual property and transported it to our adversaries.

Additionally, while the Department adopted a new conflict of interest policy in December 2021, the Notice of Proposed Rulemaking process for adopting formal conflict of interest/commitment language has been going on for several years and has not concluded. The anticipated completion date is now Spring 2025. This effort builds on formalizing the provisions laid out in the Financial Assistance Letters addressing conflicts of interest and commitment among Department funding recipients. With ever increasing funding being dedicated to promoting the research and development of emerging and critical technologies, this process needs to be completed.

Many challenges remain for the Department to fully implement National Security Presidential Memorandum 33, which requires, among other things, that the Department create a standardized set of required certifications and disclosures for all funding applicants. Such standardized language would aid in preventing foreign actors from illicitly obtaining Department intellectual property, and it would give the OIG a stronger basis to successfully prosecute offenders.

Accessing Data for the Purpose of Running Data Analytics

"The goal is to turn data into information and information into insight."

– Carly Fiorina, Former Chief Executive Officer, Hewlett Packard

Photo courtesy of Shutterstock, 2024

Significance of the Issue – Data Analytics

The use of data analytics[6] allows an organization to evaluate transactional data in support of decision-making regarding policy, program operations, resource allocations, risk management, and mission outcomes. Most importantly for the Department, data analytics is fast becoming the cornerstone of fraud detection, waste detection, and payment integrity. The Department's slow pace to utilize a data-driven approach could cost the taxpayers a substantial amount of money in the long term.

In March 2024, we issued Special Report, *The Department of Energy's Considerations and Use of Data Analytics* (DOE-OIG-24-14). This report describes the legal and policy landscape, leading practices, and past oversight recommending that the Department act. The report states the growing urgency to implement effective data analytics to improve the efficiency, economy, and effectiveness of the Department's oversight and management of its programs and operations. The report highlights that the Department's distributed and decentralized environment further exacerbates already existing data access and management challenges that hinder its ability to provide effective oversight and detect fraud, enhance data-driven management, realize performance improvement, and reduce risk to Federal resources.

It is imperative that Department leadership emphasize the collection and use of high-quality, well-managed data to address these challenges. Doing so would allow the Department to much more effectively manage the strategic risks while supporting the development of useful and timely metrics to ensure better outcomes. By prioritizing the use of data analytics, officials could also improve the Department's oversight of the more than $500 billion of risk associated

[6] Data analytics is the application of data science to draw insights from data. It is foundationally enabled by data governance, management, technical infrastructure, and data literacy across the workforce.

with the authorized or appropriated funds and loans under the IIJA, IRA, CHIPS Act, and the Puerto Rico Energy Resilience Fund.

Department Progress – Which Includes Taking Preliminary Steps to Expand Staffing Resources

The Department has taken preliminary steps toward using data analytics in its operations. For instance, the Department continues to enhance data literacy and data collaboration amongst key stakeholders within the financial community, including the Chief Data Officer, through knowledge sharing of best practices and with private industry communities. The Department has also expanded data analytics staffing resources, including contract data analysts and upskilling existing staff with training that focuses on data visualization, analytics, and science. With respect to new appropriations, the Department has launched the Lifecycle Spending Dashboard that uses interactive visualizations to track and report IIJA and IRA fund execution.

The Department has also established 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.

In addition, the Department's Data Analytics Working Group has 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 Chief Data Officer has made progress on the Department's Data Strategy and Implementation Roadmap and has reinvigorated enterprise data governance and Department-wide collaboration and information sharing on data management and governance efforts.

Several promising aspirational initiatives are underway across the Department's sites and programs, which are, of course, disconnected from any enterprise or federated strategy or approach. The Department would be well served to take advantage of these efforts to build toward a truly federated enterprise.

Challenges – Which Include Substantially Lagging on Completion and Integration of Actions Outlined in the Federal Data Strategy

In the OIG's Special Report, *The Department of Energy's Considerations and Use of Data Analytics* (DOE-OIG-24-14), we outline three considerations to which the Department concurred. These considerations included: (1) develop and implement a data governance structure, strategy, implementation plan, and capstone policy, including identifying a portfolio of high-priority, high-value use cases; (2) assess and identify resource needs, including policy, process, workforce, and information technology; and (3) adopt a coordinated approach for establishing and enforcing common minimum data standards, access to authoritative data, and accountability on implementation via transparency and consistent contract language.

We highlight progress on the first item. Programs and sites do appear to be allocating resources toward data management and analytics, but they continue to do so in a mostly distributed and decentralized manner. In the OIG's Special Report, *The Department of Energy's Considerations and Use of Data Analytics* (DOE-OIG-24-14), we report initial progress within NNSA toward developing financial data and information sharing standards. However, at the Department level, while there is some progress, much more is needed to strengthen the Department's governance and management to develop common minimum standards. In the meantime, the Department's federated governance will need to be further strengthened to support timely, effective, economical, and efficient implementation of such standards.

The Department is also substantially 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.

Playing a Leadership Role – Artificial Intelligence

"Artificial intelligence is an innovative technology that can help unleash breakthroughs in energy technologies and enhance our national security."

– Jennifer Granholm, Secretary of Energy

Photo courtesy of Shutterstock.com, 2024

Significance of the Issue – Artificial Intelligence

The rapid advancement of AI technologies, including generative AI, machine learning, and intelligent autonomous agents, presents immense opportunities and significant challenges. Nation-states vie for dominance, and unlike physical sciences, the center of mass is with American industry. Over the past year, we have witnessed the emergence of increasingly sophisticated and capable AI systems and basic AI research and techniques.

The rate of change and the resulting threats and opportunities are increasing, moving much faster than the speed of Government. This is being driven by a breathtaking amount of capital investment by the private sector, supported by high valuations in the capital markets. The implications for U.S. national security, including energy security, nuclear security, and economic competitiveness are profound and compounding. With its critical missions in energy and nuclear security, the Department must navigate this complex landscape, ensuring the safe and secure development and deployment of AI technologies.

With its extensive research, engineering, and production capabilities, the Department could be positioned to provide leadership in AI development and deployment both on the research and security side.

Department Progress – Which Includes Making Strides in Establishing an AI Governance Framework

This year, the Department has made some progress in establishing AI governance structures and promoting responsible AI use. Work across Department sites and programs, taken individually, continues to push the boundaries of AI work. However, this accelerating pace of AI development requires a renewed focus on strengthening governance, enhancing data management, and addressing ethical and security concerns as an enterprise. The Department must address these challenges, including hard questions about its ability to meet the moment with a 20th century operating and management culture. It is reasonable to ask if the Department's distributed and decentralized culture, dating back to the Manhattan project and solidified in the last century, is ready for this challenge.

The Department has made strides in establishing an AI governance framework. The adoption and expansion of the Cyber and IT/OT Executive Council and AI Advancement Council are noteworthy. The AI Advancement Council serves as the principal forum for collaboration and oversight of AI activities within the Department, providing strategic direction and addressing policy conflicts. Working groups covering topics such as AI rights, safety, and cybersecurity are underway. The appointment of a Chief AI Officer and a Responsible AI Official further strengthens the Department's AI governance structure, promoting comprehensive oversight of AI coordination, innovation, risk management, and deployment.

The Department is also engaged on the potential risks and concerns related to AI use, prioritizing responsibility, transparency, and ethical considerations in AI development and deployment. The Department produced an *AI Risk Management Playbook*, which identifies over 100 risks and mitigation techniques for AI use cases. The Department is also enhancing its cybersecurity infrastructure to address AI-specific threats and is beginning to implement best practices for secure coding, data handling, and access controls. Further, the Department is working to harmonize AI regulations, guidelines, and frameworks to ensure consistency and reduce barriers, thereby aligning legal frameworks, ethical standards, safety protocols, and data governance practices.

The Frontiers in Artificial Intelligence for Science, Security, and Technology initiative, which will engage offices across the Department and all 17 National Laboratories, signals a commitment to integration. The Department is also working to remove barriers by addressing issues such as access to AI tools, data quality, and infrastructure challenges. Efforts include securing hardware for AI development and partnering with cloud service providers to offer the latest AI services.

The Department has also stressed the need for prioritizing the recruitment, training, and retention of AI talent, updating position descriptions, leveraging AI-focused training programs, and establishing role-based AI training tracks to build AI literacy and expertise across the Department.

Challenges – Which Include Needing a Roadmap for AI Implementation

The Department must continue to address challenges associated with AI governance and should ensure that it aligns and integrates its data management and governance activities with its AI activities under a governance framework. The Department should enhance data access and usability and develop a comprehensive framework and roadmap for AI implementation that addresses ethical, security, and use concerns to meet the changes brought on by the rapid development of AI technologies. These efforts will require a proactive approach to ensure the Department remains at the forefront of innovation and safeguards its critical missions.

A comprehensive governance framework that guides the development and deployment of AI technologies should include defined roles and responsibilities. These roles and responsibilities will be essential for establishing a robust AI governance framework that fosters accountability and promotes responsible AI use. The roles and responsibilities should encompass all parts of the Department enterprise so that issues of proper AI use permeate throughout the entire agency.

The Department should also ensure it appropriately addresses the challenge of leveraging the work done by the National Laboratories and the Office of Critical and Emerging Technologies to integrate AI into the Department's daily workflow and processes more broadly. This can lead to increased efficiency and innovation. The Department can encourage consistent and effective AI implementation by developing common standards, promoting best practices, and mitigating potential risks. These standards should cover topics such as data privacy, security, ethics, and accountability, which together can provide a solid foundation for responsible AI use.

The Department must also consider and plan for how it will address possible challenges and risks related to AI use. The guidelines that are developed should be clear to aid researchers and users when developing and using AI. Prioritizing responsibility, transparency, and ethical considerations in AI development and deployment will foster trust, ensure fairness, and promote the responsible use of AI technologies. AI safety and security are dynamic areas that make it essential, especially in light of Nation-state competition and the cautionary warnings of industry, to establish data-driven linkages to enable the Department to become a timely learning organization. This could include the establishment of common minimum standards for AI-related meta-data and performance indicators to support roll-up into compelling dashboards that support identification of challenges and opportunities and more rapid cycles of learning and dissemination of leading practices.

Effective enterprise data access, management, and governance are critical enablers for AI success. Data that is accessible, authoritative, and organized is the precursor for successful AI efforts that lead to the most accurate insights. Initiatives like EDISON and Project Alexandria[7]

[7] EDISON, launched by the OCIO, is a multi-tenant data platform that will be available across the enterprise and will accelerate the path to advanced data and analytics capabilities while consolidating standard foundational data and platform management activities. Project Alexandria is leveraging existing national laboratory capabilities to develop and implement a virtual platform to store, catalog, and organize the NNSA's non-proliferation research data to improve access and discovery, promote reuse, and enable critical research.

play critical roles in improving data access, breaking down data silos, and promoting collaboration. While these efforts are promising, there is still a need for an enterprise data management system, including a catalog, shared taxonomy, and metadata management processes and standards, to support AI development and deployment. These data management and governance investments will form a solid foundation for AI applications. Including the Frontiers in Artificial Intelligence for Science, Security, and Technology, these efforts when combined with the development of a comprehensive enterprise data strategy could improve data quality, governance, and accessibility—critical components for AI training and model development.

Because of the Department's contractors' extraordinary technological expertise, it has a unique opportunity to be a leader in responsible AI development and deployment. By proactively addressing the challenges of governance, data access, and ethical considerations, and fostering a culture of innovation and collaboration, the Department may unlock the potential of AI in a safe, secure, and equitable manner. A proactive plan and well-defined framework will foster transparency, accountability, and continuous improvement in the Department's AI initiatives. Without the proper support and better integration and alignment across current efforts, the Department may lack an environment that encourages innovation and the successful use of AI technologies.

STATUS OF OTHER MANAGEMENT CHALLENGES DISCUSSED IN PREVIOUS REPORTS

Restoring Plutonium Pit Production Capability – National Nuclear Security Administration

"Bottom line, re-establishing plutonium pit production is a 'must do' and is foundational to stockpile modernization."

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

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[8] (WR) ppy.

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 – Which Includes Issuance of Awards for Glovebox Procurements at LANL and Preparations for Glovebox Installation at SRS

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, NNSA was able to provide the OIG with a status update on its pit production effort.

According to NNSA officials, 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, PF-4 must

[8] WR pits have been certified to meet the stringent quality assurance requirements necessary to enter the U.S. nuclear weapons stockpile.

expand its existing capacity. To expand capacity, LANL must decontaminate, demolish, and remove old equipment and install new equipment in conjunction with building pits in PF-4. According to NNSA officials, PF-4 is on track to have its first fully qualified pit, the "first production unit," in calendar year 2024. In addition, awards have been issued for all PF-4 glovebox procurements; however, glovebox production has been slower than expected with vendors taking 2 years to produce a glovebox. The bulk of equipment is expected to arrive next year.

At SRS, NNSA officials stated that work is ahead of schedule for preparing the SRPPF for gloveboxes. This work includes repurposing the Mixed Oxide Fuel Fabrication Facility by removing coatings and placing holes in the walls in preparation for glovebox installation. However, this schedule is based on an informal schedule to track some of the site work prior to moving into Critical Decision-2 (CD-2) where an earned value management system will be put into place allowing for a far more detailed schedule to completion. Although the cost and schedule for the SRPPF remains uncertain until CD-2 is reached, according to a 2023 fact sheet, NNSA has determined that producing 50 ppy by 2030 at SRS to meet the overall 80 ppy objective is not achievable. To produce WR pits at the required rate necessitates: (1) completing SRPPF construction and receiving startup authorization; (2) demonstrating a WR-quality pit manufacturing capability; and (3) demonstrating the ability to manufacture at full rate capacity while maintaining WR quality. After construction is finished, NNSA may need several years for the SRPPF to receive approval to begin "hot" operations and ramp up to the full rate of pit production.

Although NNSA will not reach the capability to produce 80 ppy by the original target date of 2030, SRPPF officials have stated that the first production unit pit is on track for 2035. However, that projection may change once SRPPF achieves 60 percent design complete, which we were informed was achieved at the end of October 2024. Subsequently, NNSA will be able to develop more accurate cost and schedule estimates as earned value management systems are implemented for the multitude of projects at the SRPPF.

Challenges – Which Include Limited Capabilities for Producing Gloveboxes and Slower Than Expected Production of Gloveboxes

The Department faces challenges in meeting its production objectives. The U.S. ceased largescale pit production in 1989, and as a result, most pits in the U.S. stockpile are more than 30 years old. In January 2023, the GAO's audit report, *NNSA Does Not Have a Comprehensive Schedule or Cost Estimate for Pit Production Capability*, states that "[re-]establishing pit production likely represents NNSA's largest investment in weapons production infrastructure to date" and recommends that NNSA develop a life-cycle cost estimate. The GAO found that NNSA had not developed either a comprehensive schedule or cost estimate that met GAO best practices. It also 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. In 2024, LANL developed a Plutonium Infrastructure Integrated Master Schedule that includes all work in PF-4. This site-specific schedule aligns all major items of equipment, minor construction, expense projects, and capital acquisition projects occurring at LANL.

Glovebox procurement challenges also exist according to NNSA officials. Gloveboxes are only manufactured by a few companies, and production has been slower than expected, in part, due to difficulties arising from COVID-19 (e.g., inflation, lack of resources, employee staffing for production, specialty vendor staff). Based on an estimate developed by the Glovebox Working Group, NNSA expected glovebox manufacturing to take 1 year, but vendors are taking 2 years to produce a glovebox. In addition, many vendors that manufactured the specialized equipment for use in gloveboxes have filed for bankruptcy, which has created further challenges for NNSA.

Other challenges include meeting key milestones on schedule. One recent design milestone involved achieving 60 percent design completion for the SRPPF project in the first quarter of FY 2025. In 2023, the Savannah River Nuclear Solutions (SRNS) *Performance Evaluation Summary* identifies that the SRNS has not been able to perform to the Performance Measurement baseline for the SRPPF. Additionally, the SRNS needed to be attentive to the design production for the SRPPF to recover and maintain the SRPPF design performance baseline. According to SRNS officials, in 2024, a new subcontractor took over responsibility for SRPPF engineering, procurement, and construction, and SRNS is working closely with the new subcontractor to refine the acquisition strategy, improve forecasting and scheduling, and streamline execution. With these changes, SRNS officials expect improvements in performance. We were informed that the SRPPF has met the October 31 60 percent design complete milestone. However, challenging milestones remain for this project, including approving CD-2 in the timeframe expected and completing an earned value management system with a far more detailed schedule for completion.

Design changes to the SRPPF are a major risk to completing the project within cost and schedule. To mitigate the risk of design changes, the SRPPF officials have requested NNSA's early approval of the facility's *Documented Safety Analysis*. By taking this action, the SRPPF design will include all the necessary safety structures, systems, and components, along with any administrative procedures necessary to run the facility in a safe and compliant manner.

Maintaining a fully qualified pit production workforce is a significant challenge for NNSA. Pit production work requires long hours in demanding environments, and retention of this skilled workforce within production operations has been a challenge. To address this challenge, NNSA has developed a Plutonium Premium Pay Program, which will work as a retention incentive program for employees working in designated facilities involved in plutonium production.

Managing Radioactive Liquid Waste – Office of Environmental Management

"Hanford's 56 million gallons of radioactive and chemical waste stored in 177 aging storage tanks represent EM's greatest environmental risk and financial liability." (April 2023)

– William "Ike" White, Former Senior Advisor for the Office of Environmental Management

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 and cost-effective 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 is responsible for a total inventory of approximately 90 million gallons of tank waste stored in aging underground tanks, which is a primary environmental risk at the three sites where it is located, namely the Hanford Site (Hanford) in Washington, SRS in South Carolina, and the Idaho National Laboratory Site (INL) in Idaho.

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 FY 2024 total environmental liability at approximately $545 billion according to the Department's FY 2024 *Agency Financial Report*.

Department Progress – Which Includes Producing the First Full Test Glass Container at the Low-Activity Waste Facility and INL's Integrated Waste Treatment Unit Resuming Operations in August 2024

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, the Department provided the following information regarding the Department's radioactive liquid waste operations at Hanford, SRS, and INL.

According to Department officials, 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," 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 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. Secretary Granholm committed to assessing the high-level radioactive waste interpretation during her

Congressional confirmation hearing in January 2021. This assessment, which was completed in December 2021,[9] concluded that the high-level radioactive waste interpretation is consistent with the law, science and data, and the recommendations of the Blue-Ribbon Commission on America's Nuclear Future. The Department has also evaluated a second waste stream (i.e., contaminated process equipment) at SRS for potential disposal at a licensed commercial facility under the high-level radioactive waste interpretation. The first shipment left SRS in March 2024. Future shipments of contaminated process equipment from SRS to a licensed commercial facility for treatment and disposal will continue as necessary.

Hanford

At the Hanford Waste Treatment and Immobilization Plant (WTP), startup and commissioning preparations are underway. In December 2023, the Department produced the first full test glass container at the Low-Activity Waste Facility, and cold commissioning is scheduled to begin in November 2024 to support commencement of radiological operations. Additionally, according to the Department, Hanford's Tank Side Cesium Removal System has staged over 500,000 gallons of low-activity tank waste in preparation to send to the Low-Activity Waste Facility.

SRS

Based on documentation from the Department, the Salt Waste Processing Facility (SWPF) initiated hot commissioning in October 2020 and began full operations in January 2021. Since the introduction of radioactive salt waste to the SWPF, the Department reported that it has processed about 7.5 million gallons of salt waste as of December 2023. According to SRS, as the SWPF increases efficiency and optimizes its operations, estimated process rates of up to 6 million gallons annually are projected as early as FY 2025 with current technologies. The goal is to continue to achieve SWPF efficiencies and further optimize its operations to possibly achieve future processing rates of up to 9 million gallons annually.

INL

INL's Integrated Waste Treatment Unit (IWTU) is expected to treat 900,000 gallons of liquid radioactive and hazardous waste stored in three stainless steel storage tanks. Department officials indicated that the IWTU 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. In October 2023 the IWTU entered an outage due to the detection of mercury during hot operations. Department officials stated that the IWTU resumed operations in August 2024. According to the Department, more than 74,000 gallons of sodium-bearing waste has been processed to date.

[9] 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.*

Challenges – Which Include Identifying Additional Treatment Options to Address Hanford's Remaining Low-Activity Inventory and Improving the Defense Waste Processing Facility's and the SWPF's Long-Term Reliability and Availability

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 radioactive waste facilities to prepare and vitrify the high-level radioactive waste for eventual final disposition. However, the Department is currently working with regulators on a direct feed approach for pretreatment of the high-level radioactive waste.

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 January 2023 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 continues to work with regulators to advance a Test Bed Initiative to sufficiently treat 2,000 gallons of tank waste for offsite immobilization in grout for disposal.

SRS

The Department reports needing to continue improving the Defense Waste Processing Facility's and the SWPF's long-term reliability and availability. According to SRS, when the Next Generation Solvent is implemented at the SWPF, it will enable processing up to 9 million gallons of waste per year. 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 the 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. In September 2024, Department officials estimated that processing the remaining tank farm liquid waste would take an additional 4–6 years. Additionally, the Department will need a pathway for the disposal of the processed waste currently stored at INL.

WATCH LIST ITEM

The OIG prepared a Watch List, which incorporates an issue that the OIG plans to include in our next Management Challenges report.

Underutilizing Enterprise Risk Management

"Thoughtfully assessing and addressing enterprise risk and placing a high value on corporate transparency can protect the one thing we cannot afford to lose: trust."

– Dale E. Jones, Chief Executive Officer, Magna Vista Partners

Photo courtesy of Shutterstock, 2024

Significance of the Issue – Enterprise Risk Management

Leaders at all levels of the Department are accountable for establishing appropriate strategic objectives and monitoring program performance against those objectives. Selection of effective outcome-oriented strategic objectives reflects a careful analysis of the characteristics of the problems and opportunities an agency seeks to influence through executing its mission, factors affecting those outcomes, and agency capacity and priorities. Enterprise Risk Management (ERM) is an effective approach to addressing the full spectrum of the Department's significant risks by understanding the combined impact of risks as an interrelated portfolio rather than addressing risks only within silos. ERM provides an enterprise-wide, strategically aligned portfolio view of organizational challenges, and enables enterprise-wide action to prioritize and manage risks to mission delivery.

While agencies cannot mitigate all risks related to achieving strategic objectives, performance goals, and program operations, they should identify, measure, and assess risks and associated measured triggers, to the extent possible. Historically, ERM practices focused on qualitative assessments and experience-based judgements; however, as the availability of data continues to increase, ERM decisions are shifting more toward quantitative decisions driven by the use of data analytics, which can introduce statistical rigor in the identification, tracking, and proactive management of risk. When well executed and properly aligned with performance and program evaluation, ERM improves agency capacity by allowing agency leaders to prioritize efforts, optimize resources, and assess changes in the environment. Although the Department considers enterprise-wide risk in its decision making, it does so in a fragmented fashion by aggregating risk identified by each program element rather than by examining risk from an enterprise-wide perspective.

Department Progress – Which Includes Issuing Guidance

The Department continues to take actions to address the large number of risks it faces. In December 2023, the Department issued its *Enterprise Risk Management: Fiscal Year 2024 Guidance* that emphasizes the synchronization of the Department's risk management, budget, and performance management activities. For example, the guidance was updated to enhance the Department's approach to evaluating cybersecurity risks in accordance with Federal requirements. The guidance also highlights the potential use of data analytics within the Department to improve the management and oversight of the significant influx of funds associated with the IIJA, CHIPS Act, and IRA. The guidance also illustrates the emerging risks related to AI, instructing organizations to recognize AI threats when conducting risk assessments and assembling their risk profiles.

The Department has also chartered the Departmental Internal Control and Assessment Review Council whose primary mission is to provide oversight of the Department's internal control program and to promote collaborative efforts to evaluate risk. The Departmental Internal Control and Assessment Review Council also constitutes the Department Senior Risk Management Council recommended by Office of Management and Budget Circular A-123 and the GAO.

In addition, the Department has taken action to increase awareness of cybersecurity risks among its management. For example, Environmental Management increased coordination between its leadership and one of its contractor's working groups to increase visibility and the understanding of cybersecurity risks. This in turn has resulted in progress being made in cybersecurity budget requests.

Further, NNSA has recently taken on a digital engineering initiative that it anticipates will not only improve the agility, responsiveness, and effectiveness of the nuclear security enterprise to perform its core missions, but also reduce risk to its programs. This should be commended. In

its execution, including its representation in the Department's Enterprise Risk Profile, NNSA's digital transformation faces challenges and opportunities, including change management risks related to moving from a distributed and decentralized culture to a federated operating and management culture.

Challenges – Which Include Gathering Insights From Individual Program Elements Rather Than Assessing Risk Holistically

The OIG has an ongoing project looking at the Department's investment in, and implementation of, enterprise-wide data analytics to identify and mitigate risk. This ongoing work has identified that the Department's fragmented fashion, in which it aggregates risks by each program element, may create blind spots in the universe of data that, if rectified, could be used to more accurately and timely identify, track, and respond to risk across the Department. Gathering insights from individual program elements rather than assessing risk holistically across the Department could miss enterprise-wide risks that, while less significant within any individual element, are more significant when viewed in the aggregate.

The OIG has also noted fragmentation issues within the complex. For example, although the Department designated the Strategic Integrated Procurement Enterprise System as the system of record for all Department elements for the award and administration of Department instruments where all pre- and post-award contract documents are to be maintained, the OIG found that this was not the case. Officials informed us that contractual information may be stored in other systems and that local Department offices can set their policies for storing procurement documentation outside of the Strategic Integrated Procurement Enterprise System. Unfortunately, having this information stored in an unknown number of locations could impact the Department's ability to fully evaluate the data for any potential procurement fraud risks. We also found similar issues with the lack of enterprise data being used to evaluate cybersecurity risks, which was discussed elsewhere in this report.

The OIG's forthcoming report will provide suggestions to the Department that, if implemented, should result in substantial improvements to management and oversight of its programs and operations through use of data-informed risk management practices.

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 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.