Office of Inspector General

OFFICE OF CYBER ASSESSMENTS AND DATA ANALYTICS

SPECIAL PROJECT REPORT

THE DEPARTMENT OF ENERGY SHOULD INVEST IN AND IMPLEMENT ENTERPRISE-WIDE DATA ANALYTICS TO IDENTIFY AND MITIGATE RISK

DOE-OIG-25-06
DECEMBER 2024

Department of Energy
Washington, DC 20585

December 4, 2024

MEMORANDUM FOR THE DEPUTY SECRETARY; ADMINISTRATOR, THE NATIONAL NUCLEAR SECURITY ADMINISTRATION; UNDER SECRETARY FOR INFRASTRUCTURE; UNDER SECRETARY FOR SCIENCE AND INNOVATION; CHIEF INFORMATION OFFICER; AND DEPUTY CHIEF FINANCIAL OFFICER

Teri L. Donaldson

FROM: Teri L. Donaldson
Inspector General

SUBJECT: Special Project Report: *The Department of Energy Should Invest in and Implement Enterprise-Wide Data Analytics to Identify and Mitigate Risk*

Purpose: The Office of Inspector General (OIG) is issuing this report to encourage the Department of Energy to invest in and implement enterprise-wide data analytics to improve its ability to identify and mitigate risk. Private sector organizations and the Department's public sector peers are modernizing risk management practices by marshalling technology and using data analytics to drive improvements. The Department should act now to implement plans and make investments to use data analytics to modernize its operations and optimize its enterprise-wide risk management practices.

Summary: Although the Department considers enterprise-wide risks in its decision making, it does so in a fragmented fashion by aggregating risks identified by each element[1] rather than by examining risks from an enterprise-wide perspective. This element-based approach, which reflects the Department's decentralized management and operating culture, yields gaps in information that could be detected with the use of enterprise-wide, data-informed analytical models and processes.[2] These information gaps create blind spots in the universe of data that, if captured, could be used to more efficiently identify, track, and respond to risks across the Department.

Furthermore, although the current, element-based approach provides some insight into field-level risks within the elements, this approach generates gaps because the enterprise-wide risk environment is multi-dimensional and extends beyond a compilation of element-based risks.

[1] Elements are comprised of field and Headquarters organizations.

[2] The Department's risk management process is described in the *Department's Enterprise Risk Management FY 2024 Guidance*. The *FY 2023 Department Agency Financial Report* also includes a description of the Department's risks.

Gathering insights from individual elements rather than assessing risks holistically across the Department could miss enterprise-wide risks that, while minimal within any individual element, are significant when viewed in the aggregate.[3] Enterprise-wide risks are increasingly significant for a variety of reasons. For example, the Department faces: (1) increasing and evolving external threats; (2) complex interactions with other Government and private sector stakeholders; (3) pressing and dynamic national security imperatives to accelerate integration of nuclear security enterprise modernization; and (4) the adoption of new missions aimed at fundamental national energy transformation[4].

Because of the increasing significance of enterprise-wide risks and the potential for information gaps in the current element-based approach, the OIG is providing prospective considerations to the Department for implementing enterprise-wide, data-informed methods to detect and address these risks.[5] Indeed, the Department's peers[6] and private industry[7] use enterprise-level, data-informed management as an accepted leading practice for enterprise risk management. As reported by Moody's Analytics:[8]

> Risk management's evolution into a data-driven function is transforming its role in business. Moving forward, [organizations] that invest in achieving this transformation will be best positioned to manage emerging risks, while also empowering business units to achieve their strategic goals.

The Department should join private industry and its public sector peers who are optimizing their risk management practices with data analytics. In doing so, the Department should integrate the data-informed approach into budget formulation and execution to ensure sufficient resources are devoted to the approach.[9] Failing to adopt and implement this suggested strategy, and continuing with the current approach, will likely result in sub-optimal outcomes and potential for overlooking and mischaracterizing enterprise risks.

The OIG has previously emphasized to the Department the benefits of integrated data analytics as a general-purpose management capability. Submissions for the fiscal year (FY) 2026 President's Budget provide an opportunity for the Department to take concrete action. Adoption

[3] *OMB Circular A-11*, July 2024, Page 771, states: "Enterprise risk management (ERM) is an effective agency-wide approach to addressing the full spectrum of the organization's significant risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos."

[4] OMB Circular A-11, July 2024, Section 230.12, states: "Activities being undertaken to accomplish goals and objectives are at an increased risk of failure when implementing strategies are formulated without identifying potential risks and without embedded mitigation mechanisms to effectively assess and manage such risks."

[5] These data-driven methods reflect the goals, objectives, and requirements of the Foundations for Evidence-Based Policymaking Act of 2018, *Public Law No: 115-435*.

[6] The OIG previously highlighted (DOE-OIG-24-14) Department of Defense (DOD) efforts to implement enterprise-wide use of data management and governance and to integrate data-informed business and operational management using enterprise data analytics. See here for a recent DOD update on these efforts.

[7] The OIG notes that the rationale for the Department's use of the management and operating contractor construct is to provide access to the best of America's knowledge, industrial capability, and talent for executing the Department's world-class science and engineering mission. This rationale extends to management and data science.

[8] *Embracing Data-Drive Risk Management in 2022*, *https://www.moodysanalytics.com/-/media/whitepaper/2021/Embracing-Data-Driven-Risk-Management-in-2022.pdf*.

[9] *OMB Memo M-16-17*, Attachment, Page 1.

of enterprise-level, data-informed risk management is required for optimal operations. Moreover, this approach provides an opportunity to maintain valuable aspects of the Department's current operating and management culture while supporting its modernization. To that end, this report makes timely considerations, starting with data and analytic capabilities and then expanding into and bridging enterprise risk management and budgeting (i.e., using a common corpus of managed and governed data, metrics, and analytic models and processes).[10]

Identifying, Prioritizing, and Managing the Department's Risks

The Department is required to identify and prioritize risks across the enterprise and characterize them by probability and potential severity. The Department does this by publishing guidance[11] to its elements, working with them to improve quality and consistency of submissions, and using a governance structure to consolidate results into a final risk profile. Each element develops its submission to identify and assess its risks.

The Department added substantial emphasis on data analytics in its most recent risk management guidance and encouraged elements to use data analytics to mitigate and reduce potential fraud, with particular emphasis on the execution of its new appropriations. The risk guidance also highlights the need for "[c]ontinuing the synchronization of the Department's Risk Profile to the Planning, Programming, Budgeting, and Execution processes to better align funding [for] needed resources during Budget Formulation." The Department should expand this emphasis from an element-based approach to a holistic, enterprise-wide approach.

The Department expresses prioritized risks in its Enterprise Risk Profile. In applying the risk management guidance, the Department assesses its profile of risks each year via a voting mechanism that evaluates risks identified through the element-based approach. The key features of the Department's annual risk assessment process are that: (1) it is driven by point-in-time data calls; (2) conditions are captured in very high-level, descriptive terms; and (3) elements are responsible for independently identifying and addressing risks. While this process benefits from the aggregation of subject matter expertise across the Department, it lacks statistical rigor in identifying and tracking risk triggers and focuses governance on element-based risk identification rather than holistic, enterprise-wide risk management.[12] Additional data collection, analysis, and consideration would significantly improve risk management processes.

For example, consider cybersecurity risk, an area where the OIG has done substantial work, and where the OIG was unable to discern a data-informed linkage from risk assessments to resource allocation in the Department's budget. For many years, the OIG has issued recommendations to the Department that are "similar in type" to prior recommendations that have been closed.

[10] *OMB Circular A-11*, Paragraph 51, discusses Department requirements to use data and analysis, enterprise risk management, and evaluation and evidence requirements, including developing analysis capability in its risk and budgeting process, and reflecting the same in submissions to the Office of Management and Budget (OMB).

[11] *Department's Enterprise Risk Management FY 2024 Guidance*.

[12] While experience and the views of senior leadership are important components of risk management, evidence-based identification and analysis of risks has been shown to be critical in overcoming intuition and statistical biases that generate overly optimistic decisions called the "Planning Fallacy" as noted in Daniel Kahneman's *Thinking: Fast and Slow*, 2011, Page 252.

In its most recent report, the OIG emphasized the Department's need to conduct analyses and take enterprise-wide actions to improve its cybersecurity posture. [13]

The Department has made substantial investments in cybersecurity directly both through its Office of the Chief Information Officer and within its elements. However, the repeated occurrence of "similar in type" findings and recommendations across the enterprise indicates a potentially unmet need to develop consistent and repeatable operational and performance measures. Adoption of data-informed measures would improve the Department's investments by making use of authoritative data to support root-cause analysis and to enable resource-aligned, performance-measured action across the Department's cybersecurity risks.

The National Nuclear Security Administration's (NNSA) commitment towards adoption of data-informed digital engineering in its effort to rebuild and recapitalize the nuclear security enterprise after decades of atrophy illustrates the potential value of data analytics to modern management. The digital transformation vision articulated by the Administrator and described in Appendix A requires timely, well-managed, and authoritative data; data management and governance; information sharing and safeguarding; common infrastructure; workforce initiatives; and data analytics. In its execution, including its representation in the Department's Enterprise Risk Profile, NNSA's digital transformation faces the same challenges and opportunities described in this memorandum, including change management risks[14] related to moving from a distributed, decentralized culture to a federated operating and management culture.[15] NNSA's efforts provide input for what the Department should consider on an enterprise-wide basis.

Risk and Data-Informed Budget Formulation

Among several thousand pages filled with summary documents, tables, and detailed volumes, the Department's *FY 2025 Budget Justification*, released on March 11, 2024, does not appear to reference the use of data-informed measures to assess and manage enterprise-wide risks. Nevertheless, the Department's internal budget guidance refers to the annual Enterprise Risk Profile and directs programs to address these risks in their budget submissions. Integrating risk data to the budget process is one way to get participation from sub-elements and from management and operating contractor partners.

Although the Department's budget includes organization-specific approaches to these topics, the OIG found limited or no discussion or references in the budget as to how sub-organizational approaches address enterprise-wide risks. For example, while NNSA's detailed FY 2025 budget justification contains discussion of its digital engineering initiative, within which NNSA discusses the centrality of its digital engineering initiative for addressing its modernization challenge, the document contains limited discussion linking digital engineering to mitigating

[13] *The Department of Energy's Unclassified Cybersecurity Program—2023*, Appendix 1, has a table summarizing "similar in type" findings for the past 3 years. The findings are tied to specific controls within the National Institute of Standards and Technology Risk Management Framework.

[14] The Department's change management risks are potentially underweighted as an artifact of the current process.

[15] NNSA's Digital Transformation Senior Steering Group recognizes cultural challenges with its digital transformation initiative. For example, the results of the 2024 Digital Engineering Workshop highlighted the work of the Culture Change Working Group.

change management or other execution risks, including core cultural and long-standing programmatic risks, even at the NNSA's sub-organizational level.[16]

The issue of cybersecurity illustrates the imperative to budget for an enterprise-wide approach to risk management. In the FY 2025 and FY 2026 President's Budgets, the Director of OMB and the National Cyber Director issued public budget guidance for cybersecurity priorities.[17] Both memoranda request agencies to address Government-wide cybersecurity risks in agency budgeting. In fact, the current guidance requires, "Agency *budget submissions* should demonstrate *how agencies are reducing risk*."[18]

For agencies with distributed and decentralized structures, OMB's current memorandum further states, "Agencies with federated networks should *prioritize investments in department-wide, enterprise solutions* to the greatest extent practicable in order to further align cybersecurity efforts, ensure consistency across mission areas, and enable information sharing."

The current guidance also adds a requirement for agencies to provide plans to implement data-driven decision that will be reviewed by the Office of the National Cyber Director, OMB, and by the Cybersecurity and Information Security Agency, along with their budget requests. The current memorandum highlights the focus on using data to link budgets to outcomes consistent with this memorandum:

> The Administration is committed to data-driven decision-making and departments and agencies are expected to incorporate performance measurement strategies into resource requests in order to build visibility in requested activities and allow effective measurement of investments.

Finally, the OIG notes that although some individuals[19] within the Department characterize aspects of the Executive Branch cybersecurity requirements as "unfunded mandates," OMB's budget, risk, and cybersecurity guidance — which requires agencies to make investments that demonstrably plan to reduce enterprise risks in its budget proposals — anticipates providing funding in the President's Budget based on specific investments to use data-informed methods to improve assessment and management of risk.

Role of Data Management, Governance, and Analytics

The OIG has identified the Department's limited use of data analytics as a management challenge for many years.[20] The OIG also recently noted in its report, *The Department's*

[16] For example, those risks are described in the Government Accountability Office's (GAO) High-Risk Listing and subsequently developed in this memorandum.

[17] *Administration Cybersecurity Priorities for the FY 2026 Budget* (M-24-14) was issued on July 10, 2024, and *Administration Cybersecurity Priorities for the FY 2025 Budget* (M-23-18) was issued on June 27, 2023, from both the Director of OMB and the National Cyber Director.

[18] Italics added to these quotes.

[19] A recent example is an *interview* by the Department's Chief Information Officer on July 8, 2024.

[20] Special Report on *Management Challenges at the Department of Energy—Fiscal Year 2022* (DOE-OIG-22-11, November 2021); Special Report on *Management Challenges at the Department of Energy—Fiscal Year 2023*.

Considerations and Use of Data Analytics (DOE-OIG-24-14, March 2024) (March 2024 OIG Report), that data is often collected and stored in various stove-piped systems and databases within the Department. The OIG observed the necessity of a cohesive, comprehensive, and governed approach to linking data, including ensuring consistent data standards and methods to support data analytics based on authoritative data.

Such an approach could provide meaningful timely enterprise-level insights and correlations that would standardize and integrate cross-functional and cross-organization information, inform decision making, drive administrative efficiencies, produce consistent element and Department reports, and improve performance. The creation of requisite standards via enterprise data management and federated support to conduct governance and analytics requires policies as well as focus on, and funding for, oversight. It also requires an enterprise data management process focused on an accurate and comprehensive inventory of data assets, aligned human capital, technical infrastructure, and appropriate secure data access. In the March 2024 OIG Report, the OIG reported that:

> Despite increased Federal efforts to promote information as a valuable national resource and strategic asset, and the progress made by comparable peers, [the Department] lacks the data and governance structure necessary to make critical decisions or gain visibility into program objectives. 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.

The OIG has also reported that the Department is under-resourced compared to its peers for oversight of its programs and operations.[21] Inspector General Teri Donaldson has underscored this point in the context of the substantial risk related to new appropriations under recent legislation.[22] In her testimony and in OIG reports, she has further highlighted the use of data analytics as an established leading practice that could improve the Department's efficiency, effectiveness, and economy generally, and help the Department address its oversight risk with new appropriations specifically. Her observations have built upon the GAO's recommendations made in 2017 that the Department adopt data analytics and set requisite common minimum standards, recommendations that continue to remain open.[23]

(DOE-OIG-23-08, November 2022); and Special Report on *Management Challenges at the Department of Energy—Fiscal Year 2024* (DOE-OIG-24-05, November 2023).

[21] Special Report on *Management Challenges at the Department of Energy—Fiscal Year 2023* (DOE-OIG-23-08, November 2022) has "demonstrated that the [Department] has the smallest acquisition workforce oversight ratios by far—a 0.2 percent rate of acquisition workforce per contract dollars in the Department as compared to the next lowest peer agency with 0.9 percent rate."

[22] *Statement From the Honorable Teri L. Donaldson, Inspector General, Department of Energy, to the U.S. House of Representatives Committee on Oversight and Accountability Subcommittee on Economic Growth, Energy Policy, and Regulatory Affairs* on April 18, 2023.

[23] *Department of Energy: Use of Leading Practices Could Help Manage the Risk of Fraud and Other Improper Payments* (GAO-17-235, March 2017).

We recognize efforts underway at the Department to increase data literacy, emphasize data quality, and understand the potential uses of data. However, Department officials have indicated that to be successful and meet Government-wide requirements, the Department needs to develop and resource formal and federated[24] data management, data governance, and data analytics functions.[25]

The Department previously concurred with OIG recommendations to: (1) strengthen its data infrastructure via a portfolio of prioritized use cases; (2) identify necessary resources; and (3) set needed, common minimum standards. The OIG suggests considering prioritizing integration of actionable, operationally useful insight—via data analytics—into highest priority risks across its enterprise risk management and budgeting processes, as a prioritized use case. Such an approach would build on and bridge the noted gap between the Department's risk and budgeting process and conform to the Department's published priorities in this area.

Separately, the Department's Chief Data Officer has reported that there is interest across the enterprise in shared and federated data management, governance, and analytics techniques, including developing requisite technical, policy, human capital, and process infrastructure. Program leaders have also highlighted a core opportunity for data analytics with program-related performance oversight and funds accountability as described in Appendix B. The Chief Data Officer has also identified promising program and site initiatives as well as reported progress towards publishing the Department's inaugural Enterprise Data Strategy[26] and associated multi-year implementation plan that addresses related policies, processes, and requisite information technology infrastructure. However, the Chief Data Officer has indicated that there are element-level concerns about the Department's commitment to fund, resource, deliver, and operate these capabilities, including basic prerequisites such as support for data cataloging and master data management.

Without clear Department guidance and resourcing that addresses enterprise commitment to, and support for, the use of data management, data governance, and data analytics, and given that risk management continues to use a compilation of element-level risks, it is unlikely that, without more, the Department's programs will self-organize or align their investments in an appropriate, coordinated, and efficient manner that measurably addresses enterprise risks.

[24] The OIG uses the working definition of federated governance in this context to have at least four characteristics: (1) diverse and representative governance body covering the required programmatic and functional scope and led by the appropriate responsible and empowered functional leader; (2) ability for this governance body, with appropriate staff and subject matter expertise support, to set required common minimum standards and/or other enforceable policies or processes to address its priority agenda items; (3) a commitment for high-quality, timely tracking and transparency of implementation of common standards, paired with a commitment to implementation and accountability via the chain of command; and (4) a transparent cycle of accountability, performance assessment, and planning using authoritative data to support organizational learning and improvement.

[25] The March 2024 OIG Report contains management concurrences with our consideration for identifying required resources. In that report, another consideration to which management concurred was to identify a portfolio of high-priority use cases aligned with the Department's missions and organizations.

[26] The Department is scheduled to publish and formalize its Enterprise Data Strategy in the fourth quarter of FY 2024. The formalization of this strategy is a statutory requirement defined in Public Law No: 115-435 on January 14, 2019.

Further, the March 2024 OIG Report stated that, without improvements to the use of data analytics, the OIG did not see a path for the Department to sufficiently enhance its operations to warrant removal from the GAO's High-Risk List. While narrowing the scope of its listing, the Department, including NNSA, has not taken comprehensive and required action in the face of decades of oversight findings,[27] legal mandates, and Executive Branch direction to address its high-risk listing. Using a repeatable, timely, data-informed approach to identifying, measuring, and managing dynamic and evolving operational and other risks within a cycle of accountability, learning, and performance improvement is a key aspect of moving from "high-risk" to just "risk." Private sector organizations and the Department's public sector peers have established modernized leading practices using information technology advances with data management and data analytics. The Department should follow their lead and adopt these practices.

To start, the Department can use the budget process to reinforce a federated enterprise vision for data management, governance, and analytics and to make corresponding infrastructure investments required to identify, measure, and address enterprise risks. The Department can set the parameters and provide transparency to ensure proper balance between its enterprise and element requirements and to derive collective benefits from respective capabilities. It can also use the coming months—before publication of the FY 2026 President's Budget—to refine its processes and proposals to ensure it is best positioned to be properly resourced and aligned to realize potential benefits in a planned and systematic manner. Doing so will also strengthen the Department's alignment with OMB guidance[28] to agencies to improve: (1) access to data and quality of data, including strengthening data infrastructure, and (2) use of authoritative analytics applied to accomplish evidence-based policymaking and management.

Call to Action:

The OIG is providing considerations to link and integrate data-driven risk management, data analytics, and the budgeting processes across the enterprise. We suggest considering: (1) starting with identification and treatment of the highest enterprise-wide risks; (2) continuing with analysis and integration of risks defined by the elements; and then (3) expanding to the execution of risk management governance practices as the underlying capabilities mature. This approach includes leveraging the Department's contractor-operated sites and its program elements, where the Department's financial and human resources are concentrated, and reviewing its alignment with OMB's published budgetary guidance among other guidance. Specifically, the Department should consider acting to:

1. Strengthen linkage from its enterprise risk management processes—including considering OIG- and other organization-identified risks—into its budget and data management processes in a systematic and quantifiable manner;

[27] The Department is referenced in the original GAO's High-Risk List for its "Contractor Oversight." The Department currently recognizes that this area continues to be a very high risk, 34 years later. See the letter to *Senator John Glenn and Congressman John Conyers, Jr., Chairmen, respectively, of the Senate Committee on Government Affairs and House Committee on Government Operations, From Comptroller General Charles Bowsher* on January 23, 1990. The Department's being a plank-holder is not a distinction of honor in this case.

[28] *Phase 1 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Learning Agendas, Personnel, and Planning Guidance* (M-19-23) and *Evidence-Based Policymaking: Learning Agendas and Annual Evaluation Plans* (M-21-27).

2. Integrate a more explicit line of sight into its budget submissions, aligned with OMB Circular A-11, for how investments across programs and operations address the highest enterprise risks, using qualitative and quantitative performance measures built on top of well-managed, authoritative data;

3. Establish and use data analytics products, as described above, to put into place the infrastructure that provides a common set of managed and governed data and resulting measures across its risk and budgeting processes, and other high-value use cases; and

4. Consider opportunities to benchmark its risk, data, analytics, and budgeting processes against public and private sector peers and use the results to inform and align specific approaches to digital transformation with the Department and NNSA.

Additionally, the Administrator, NNSA, should consider opportunities to:

5. Leverage, inform, and align NNSA's digital transformation with the Department's efforts.

Possible Approach:

The Department's leaders should be charged with integrating federated data management, data governance, and data analytics approaches more explicitly, starting with the Department's and NNSA's FY 2026 budget process. The approaches should align with the considerations in the March 2024 OIG Report and the discussion of the Department's risk management and budgeting processes described in this memorandum, and other priority use cases, as described in the March 2024 OIG Report.

The integrated treatment of federated data and analytics may include asking programs to clearly delineate, among other things: (1) data management and related (i.e., data governance) analytics proposed spending; (2) targeted capabilities, use cases, and performance improvements, including risk management; (3) needed contractual and/or financial assistance terms and conditions changes; (4) known top data governance and data management risks and opportunities; and (5) alignment with pertinent Department strategies and guidance.

Doing so will facilitate a systemic and holistic approach with required investments in policy and process, data management and governance, data analytics, workforce, and technical infrastructure. This treatment will also ensure identification and curation of clearly defined and sponsored high-value use cases to measure the near- and mid-term results. Finally, it will allow the Department to consider its highest priority risks and challenges in its ongoing budget formulation process and to demonstrate performance-measurable progress towards managing and buying down those risks and challenges.

Management Comments:

Management stated that the Department’s enterprise risk management and internal control program integrates and consolidates risk identified by Department Elements. The resultant risks are considerations for funding priorities with Department Elements’ budgets, and the Department’s budget reflects the priorities of Department leadership. Management also commented that as the Department implements initiatives to expand the use of data analytics within the enterprise risk management, internal control, and budget processes, it will continue to consider and determine future enhancements and beneficial applications of data analytics across the Department to further integrate risk management at the enterprise level. Management’s comments are included in Appendix 4.

Office of Inspector General Response:

For several years, the OIG has identified the need for the Department to enhance its use of data analytics. While the Department has taken some incremental steps, the Department has not embraced an enterprise-wide strategy for the use of data. For this reason, the Department is not fully informing its risk management, internal controls, and budget processes.

Appendix 1: Digital Transformation of the Nuclear Security Enterprise

While undergoing a major expansion of scale and complexity of its operations via seven simultaneous weapons system modernization activities, the National Nuclear Security Administration (NNSA) is moving towards adopting and using data-informed processes. The expansion results from a need to rebuild and recapitalize the nuclear security enterprise after decades of atrophy to meet national security requirements.[29] In part because NNSA represents about one-half of the Department's base appropriations, its broad activities—including modernization—carry substantial risk.[30]

NNSA is using digital engineering, among other things, to manage these risks. When discussing modernization of the nuclear security enterprise, Administrator Jill M. Hruby stated:

> A top priority initiative is digital engineering. We are standing up an enterprise-wide classified collaborative computing environment along with a repository of digital product information. The digital engineering effort aims to fully enable digital engineering for the W93 program, but earlier modernization programs will benefit as it progresses. This initiative is especially important because it accelerates our ability to communicate seamlessly between design and production agencies, apply [artificial intelligence] to improve production processes, identify and assess anomalies in testing, predict aging effects from surveillance data, and inform future designs. [31]

NNSA thus recognizes the role of digital engineering, knowledge management, and supporting secure technical infrastructure to support this expansion effectively, economically, and efficiently. Together, this emphasis on digital transformation across the nuclear security enterprise is aimed at synchronizing activities, discovering and integrating efficiencies, managing risk and change, and supporting agile operations.

Indeed, NNSA is looking to better synchronize activities across the nuclear security enterprise through digital transformation and across a single enterprise blueprint to "help reinforce NNSA's underlying philosophy of responsiveness, flexibility, and resiliency required to meet dynamic demands."[32] NNSA's digital transformation vision is consistent with this memorandum's emphasis on the value of data management and data analytics, and corresponding emphasis on culture and risk management adaptation. NNSA's vision suggests a commitment towards a more federated, data-driven management of operational, performance, and strategic risk; learning through enterprise-wide use of data analytics powered by effective data management and governance; aligned workforce initiatives; shared technical infrastructure; and information sharing and safeguarding. The Department should consider a similar commitment.

[29] *A New Foundation for the Nuclear Enterprise Report of the Congressional Advisory Panel on the Governance of the Nuclear Security Enterprise* by Norman R. Augustine, Admiral Richard W. Mies, U.S. Navy (Retired), et al.
[30] Secretary of Energy Jennifer M. Granholm's and Administrator Jill M. Hruby's *Testimony Before the Senate Committee on Armed Services* on April 17, 2024.
[31] *NNSA Administrator Jill Hruby Remarks at Strategic Weapons in the 21st Century Symposium* on April 18, 2024.
[32] Ibid.

Appendix 2: Benefits Accessible to the Department of Energy from Use of Data Analytics

A focus on coordinated integration and enterprise-wide use of data analytics, including artificial intelligence, can reduce overlap of program office efforts and increase their consistency. It can further enable, with maturation, enterprise-wide and data-driven approaches to:

- Strengthen integrated identification, and accelerate addressing of, enterprise risks through enterprise-wide risk management governance plans, standard operating procedures, and higher-fidelity linking of data and risks across programs and sites;

- Move towards earlier detection and prevention of fraud, waste, and abuse with process and risk-model improvement, by using automated and timely Department monitoring of authoritative financial data and performance data in internal control testing;

- Improve allocation and management of resources by engaging end users in modernizing core financial data and performance data collection tools and by ensuring consistent use of authoritative, quality data;

- Support faster, deeper, and blended policy analysis and operational decision making by enabling program offices to include any desired program-specific data within the Department's financial systems for improved downstream project monitoring;

- Allow for quicker, higher-fidelity evidence-building and program evaluation through standard data dictionaries, naming conventions, and field formats to map data outputs;

- Establish governed, authoritative enterprise data catalogs, sharing, reporting, and analytical products for high-value use cases;

- Streamline and reduce the administrative burden associated with producing Department reports while increasing quality and consistency;

- Align and deepen measurements of organizational performance by establishing and monitoring financial, operational compliance-related, and operational performance metrics and key performance indicators; and

- Develop actionable insight more quickly on Department and program goals and priorities to include benchmarking of Federal and industry best practices in financial, performance, and operational management.

Appendix 3: Methodology

This Special Project Report was developed under the authority granted by the Inspector General Act (5 U.S.C. § 406(a)(2)) to report on matters related to Department of Energy programs and operations that, "in the judgement of the Inspector General," are necessary or desirable. The work was conducted in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Federal Offices of Inspector General*, which sets forth the overall quality framework for managing, operating, and conducting the work of Offices of Inspectors General. To accomplish our purpose, we:

- Developed this report using agile oversight methods supported by the Council of the Inspectors General on Integrity and Efficiency.

- Reviewed Department guidance covering budget development and justifications, enterprise risk management, data management, and the annual *Agency Financial Report*. Assessed these documents to determine gaps among the Department's risk, budget, and data management processes based on Office of Management and Budget guidance and mandates, relevant statutes, and both government and industry best practices.

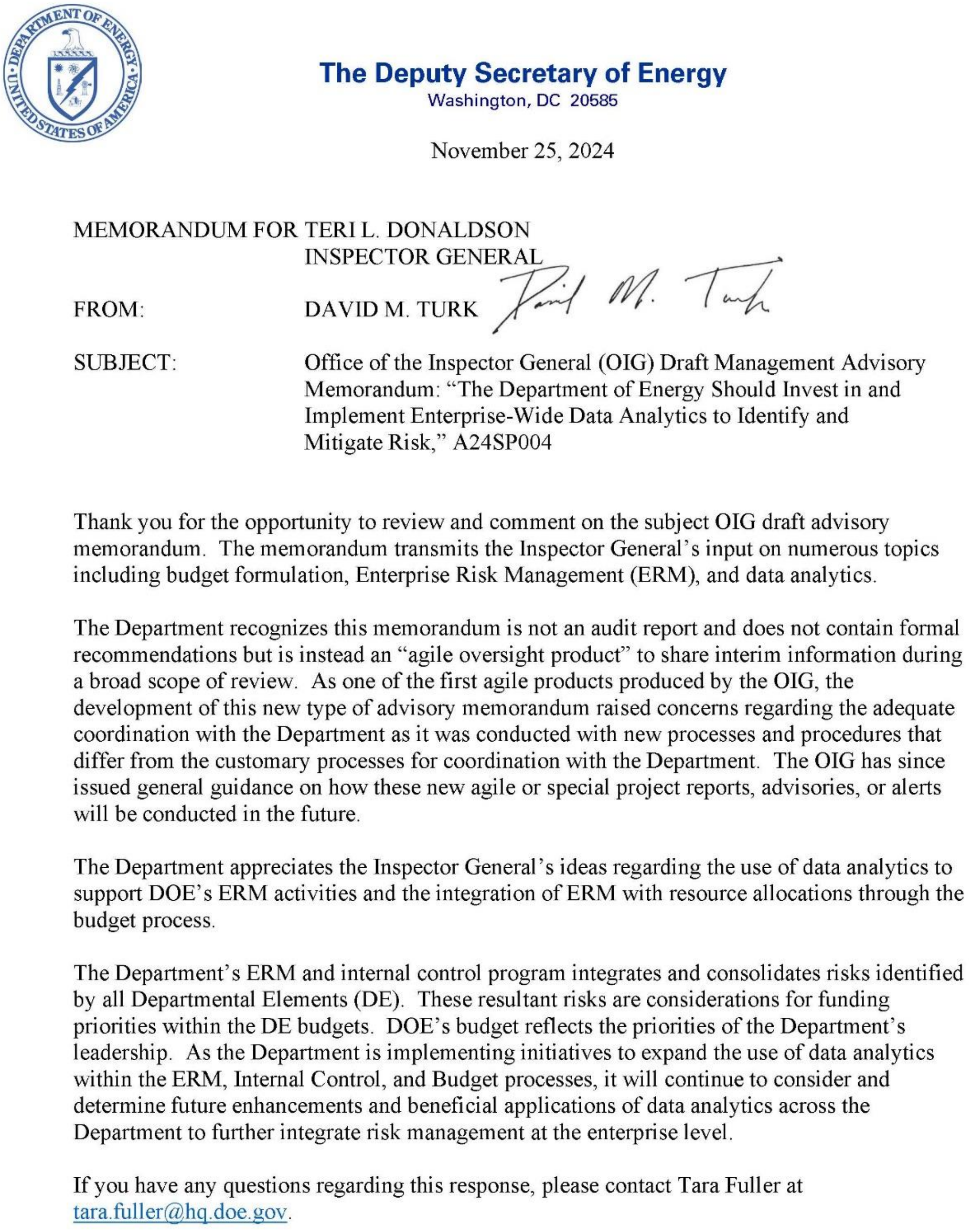
- Reviewed Office of Inspector General audits and investigations over the past 5 years to identify common risks or deficiency incidents that, when viewed collectively, could represent a higher degree of risk at the Department level.

- Identified potential gaps in Department oversight of its programs and operations that could occur when it did not align risk, budget, and data management processes.

- Discussed our concerns with Department officials and staff ahead of issuing this memorandum so that the Department could begin to narrow those gaps in the current budget cycle.

- Provided the Department the opportunity to review preliminary drafts of this memorandum and, based on feedback provided by the Department, made appropriate revisions to the memorandum.

Appendix 4: Management Comments



The Deputy Secretary of Energy
Washington, DC 20585

November 25, 2024

MEMORANDUM FOR TERI L. DONALDSON
INSPECTOR GENERAL

FROM: DAVID M. TURK David M. Turk

SUBJECT: Office of the Inspector General (OIG) Draft Management Advisory Memorandum: "The Department of Energy Should Invest in and Implement Enterprise-Wide Data Analytics to Identify and Mitigate Risk," A24SP004

Thank you for the opportunity to review and comment on the subject OIG draft advisory memorandum. The memorandum transmits the Inspector General's input on numerous topics including budget formulation, Enterprise Risk Management (ERM), and data analytics.

The Department recognizes this memorandum is not an audit report and does not contain formal recommendations but is instead an "agile oversight product" to share interim information during a broad scope of review. As one of the first agile products produced by the OIG, the development of this new type of advisory memorandum raised concerns regarding the adequate coordination with the Department as it was conducted with new processes and procedures that differ from the customary processes for coordination with the Department. The OIG has since issued general guidance on how these new agile or special project reports, advisories, or alerts will be conducted in the future.

The Department appreciates the Inspector General's ideas regarding the use of data analytics to support DOE's ERM activities and the integration of ERM with resource allocations through the budget process.

The Department's ERM and internal control program integrates and consolidates risks identified by all Departmental Elements (DE). These resultant risks are considerations for funding priorities within the DE budgets. DOE's budget reflects the priorities of the Department's leadership. As the Department is implementing initiatives to expand the use of data analytics within the ERM, Internal Control, and Budget processes, it will continue to consider and determine future enhancements and beneficial applications of data analytics across the Department to further integrate risk management at the enterprise level.

If you have any questions regarding this response, please contact Tara Fuller at tara.fuller@hq.doe.gov.

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.