



441 G St. N.W.
Washington, DC 20548

May 29, 2025

Ms. Dawn Zimmer
Acting Chief Information Officer
U.S. Department of Energy
1000 Independence Ave., SW
Washington, DC 20585

Chief Information Officer Open Recommendations: Department of Energy

Dear Ms. Zimmer:

I am writing to you with respect to your role as the Acting Chief Information Officer (CIO) for the Department of Energy (Energy). As an independent, non-partisan agency that works for Congress, GAO's mission is to support Congress in meeting its constitutional responsibilities and help improve the performance and ensure the accountability of the federal government. Our work includes investigating matters related to the use of public funds, evaluating programs and activities of the U.S. Government at the request of congressional committees and subcommittees or on the initiative of the Comptroller General, and as required by public laws or committee reports. Our duties include reporting our findings and recommending ways to increase economy and efficiency in government spending. The purpose of this letter is to provide an overview of the open, publicly available GAO recommendations to Energy that call for the attention of the CIO.

We identified recommendations that relate to the CIO's roles and responsibilities in effectively managing IT. They include strategic planning, investment management, and information security. We have previously reported on the significance of the CIO's role in improving the government's performance in IT and related information management functions.¹ Your attention to these recommendations will help ensure the secure and effective use of IT at the department.

Currently, Energy has nine open recommendations that call for the attention of the CIO. Each of these recommendations relates to a GAO High-Risk area: (1) [Ensuring the Cybersecurity of the Nation](#) and (2) [Improving IT Acquisitions and Management](#).² In addition, GAO has designated two of the nine as priority recommendations.³ Fully implementing these open recommendations

¹See for example, GAO, *Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities*, [GAO-18-93](#) (Washington, D.C.: Aug. 2, 2018).

²GAO, *High-Risk Series: Heightened Attention Could Save Billions More and Improve Government Efficiency and Effectiveness*, [GAO-25-107743](#) (Washington, D.C.: Feb. 25, 2025).

³Priority recommendations are those that GAO believes warrant priority attention from heads of key departments or agencies. They are highlighted because, upon implementation, they may significantly improve government operations, for example, by realizing large dollar savings; eliminating mismanagement, fraud, and abuse; or making progress toward addressing a high-risk or duplication issue. Since 2015 GAO has sent letters to selected agencies to highlight the importance of implementing such recommendations.

could significantly improve Energy's ability to deter threats and manage its critical systems, operations, and information. I have summarized the nine recommendations here. See the enclosure for additional details on these recommendations.

Ensuring the Cybersecurity of the Nation. Energy needs to take additional steps to secure the information systems it uses to carry out its mission. For example, we recommended that Energy develop a cybersecurity risk management strategy to protect the department against cyber threats. Until Energy implements this recommendation, the department may lack a clear organization-wide understanding of acceptable risk levels and appropriate risk response strategies to protect its systems and data.

In addition, we recommended that the department fully implement all event logging requirements as directed by the Office of Management and Budget (OMB). Until Energy does so, there is increased risk that the department will not have complete information from logs on its systems to detect, investigate, and remediate cyber threats.

Improving IT Acquisitions and Management. Energy needs to improve its acquisition of cloud services and manage software licenses more efficiently. In particular, four recommendations concern addressing key OMB cloud procurement requirements. For example, we recommended that the CIO develop guidance regarding standardizing cloud service-level agreements. Implementing this recommendation would help ensure that Energy is consistently holding its cloud providers accountable for their service performance.

In addition, we have two recommendations related to Energy's management of its software licenses. For example, we recommended that the department implement procedures for comparing its inventories of active software licenses to purchased licenses to identify opportunities to reduce cost and improve investment decisions. Until Energy does so, the department will be hindered in its ability to identify areas of duplication and cost savings for its IT assets and to optimize resource allocation.

Further, we recommended that Energy complete annual reviews of its IT portfolio consistent with federal requirements. Until Energy implements this recommendation, investments with substantial cost, schedule, and performance problems may continue unabated without necessary corrective action.

Copies of this letter are being sent to the appropriate congressional committees and the Federal CIO. The letter will also be available at no charge on the GAO website at <https://www.gao.gov>. In addition, we sent a separate letter related to agency-wide priority recommendations, which discusses the importance of addressing cybersecurity risks, to the Secretary of Energy.⁴ We are also sending a letter on open recommendations and key issues related to financial management to Energy's Chief Financial Officer.

If you have any questions or would like to discuss any of the recommendations outlined in this letter, please do not hesitate to contact me at marinosn@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this letter. Our

⁴GAO, *Priority Open Recommendations: Department of Energy*, [GAO-25-108093](#) (Washington, D.C.: Apr. 11, 2025).

teams will continue to coordinate with your staff on addressing these nine open recommendations that call for the attention of the CIO. I appreciate Energy's continued commitment and thank you for your personal attention to these important recommendations.

Sincerely,

//SIGNED//

Nicholas Marinos
Managing Director
Information Technology and Cybersecurity

Enclosure

cc: Mr. Greg Barbaccia, Federal CIO, Office of Management and Budget

Enclosure

Chief Information Officer Open Recommendations to the Department of Energy

This enclosure includes the open, publicly available GAO recommendations to the Department of Energy (Energy) that call for the attention of its Chief Information Officer (CIO). We have divided these recommendations into two categories: (1) ensuring the cybersecurity of the nation and (2) improving IT acquisitions and management.

Ensuring the Cybersecurity of the Nation

Federal agencies depend on IT systems to carry out operations and process, maintain, and report essential information. The security of these systems and data is vital to protecting individual privacy and ensuring national security. Table 1 provides information on the open cybersecurity-related recommendations relevant to the Energy CIO.

Table 1: Open Chief Information Officer-related Cybersecurity Recommendations for the Department of Energy (Energy)

| GAO report number | GAO report title | Recommendation |
|-------------------------------|---|---|
| GAO-19-384 | Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges | The Secretary of Energy should develop a cybersecurity risk management strategy that includes the key elements identified in this report. (Recommendation 8)* |
| GAO-24-105658 | Cybersecurity: Federal Agencies Made Progress, but Need to Fully Implement Incident Response Requirements | The Secretary of Energy should ensure that the agency fully implements all event logging requirements as directed by Office of Management and Budget guidance. (Recommendation 4) |

Source: GAO summary based on previously issued reports. | GAO-25-108404

*Indicates a priority recommendation.

Improving IT Acquisitions and Management

Federal IT investments too frequently fail to deliver capabilities in a timely, cost-effective manner. Key management challenges—such as a lack of disciplined project planning and program oversight—continue to hamper effective acquisition and management of the government’s IT assets. Table 2 provides information on the open IT acquisition and management-related recommendations relevant to the Energy CIO.

Table 2: Open Chief Information Officer (CIO)-related IT Acquisition and Management Recommendations for the Department of Energy (Energy)

| GAO report number | GAO report title | Recommendation |
|-------------------------------|---|---|
| GAO-24-105717 | Federal Software Licenses: Agencies Need to Take Action to Achieve Additional Savings | <p>The Secretary of Energy should ensure that the agency consistently tracks software licenses that are currently in use for its widely used licenses by, at a minimum, consistently implementing its procedures for tracking license usage. (Recommendation 3)</p> <p>The Secretary of Energy should ensure that the agency consistently compares the inventories of software licenses that are currently in use with information on purchased licenses to identify opportunities to reduce costs and better inform investment decision making for</p> |

| GAO report number | GAO report title | Recommendation |
|-------------------|--|--|
| GAO-24-106137 | Cloud Computing: Agencies Need to Address Key Office of Management and Budget (OMB) Procurement Requirements | <p>its widely used licenses on a regular basis. At a minimum, it should consistently implement its procedures for comparing the inventories of licenses in use to purchase records. (Recommendation 4)*</p> <p>The Secretary of Energy should ensure that the CIO of Energy develops guidance to put a cloud service level agreement (SLA) in place with every vendor when a cloud solution is deployed. The guidance should include language that addresses the OMB four required elements for SLAs, including: continuous awareness of the confidentiality, integrity, and availability of its assets; a detailed description of roles and responsibilities; clear performance metrics; and remediation plans for non-compliance. (Recommendation 8)</p> <p>The Secretary of Energy should ensure that the CIO of Energy develops guidance regarding standardizing cloud SLAs. (Recommendation 9)</p> <p>The Secretary of Energy should ensure that the CIO of Energy develops guidance to require that contracts affecting the agency's high value assets that are managed and operated in the cloud include language that provides the agency with continuous visibility of the asset. (Recommendation 10)</p> <p>The Secretary of Energy should ensure that the CIO of Energy updates its existing contracts for high value assets that are managed and operated in the cloud to meet OMB's requirement once guidance from the CIO Council is available on language that provides the agency with continuous visibility of the asset. If modifying the existing contract is not practical, the agency should incorporate language into the contract that will meet OMB's requirement upon option exercise or issuance of a new award. (Recommendation 11)</p> |
| GAO-25-107041 | IT Portfolio Management: OMB and Agencies Are Not Fully Addressing Selected Statutory Requirements | <p>The Secretary of Energy should direct the department CIO to work with OMB to ensure that annual reviews of their IT portfolio are conducted in conjunction with the Federal CIO and the Chief Operating Officer or Deputy Secretary (or equivalent), as prescribed by the Federal Information Technology Acquisition Reform Act. (Recommendation 15)</p> |

Source: GAO summary based on previously issued reports. | GAO-25-108404

*Indicates a priority recommendation.

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [X](#), [LinkedIn](#), [Instagram](#), and [YouTube](#).
Subscribe to our [Email Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

Automated answering system: (800) 424-5454

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

A. Nicole Clowers, Managing Director, CongRel@gao.gov

General Inquiries

<https://www.gao.gov/about/contact-us>

