INSPECTOR GENERAL

UNITED STATES OF AMERICA
FEDERAL LABOR RELATIONS AUTHORITY
WASHINGTON, D.C. 20424-0001

MEMORANDUM

DATE: September 15, 2025

TO: Colleen Duffy Kiko
Chairman

Anne M. Wagner
Member

FROM: Dana Rooney *Dana Rooney*
Inspector General

SUBJECT: Top Management and Performance Challenges for Fiscal Year 2026 (MC-25-01)

Each Inspector General is required by the Reports Consolidation Act of 2000[1] to provide the agency head with a statement that "summarizes what the inspector general considers to be the most serious management and performance challenges facing the agency" and "briefly assesses the agency's progress in addressing those challenges."[2] The law states that the "agency head may comment on the inspector general's statement, but may not modify the statement."[3] The Inspector General's statement must be included in the Federal Labor Relations Authority's (FLRA) annual Performance and Accountability Report (PAR) or Agency Financial Report for Fiscal Year (FY) 2025.[4]

The FLRA Inspector General's statement is based on the Office of Inspector General's (OIG) experience and observations from our oversight work, as well as our general knowledge of the FLRA programs and operations. In the statement for this year, we identified three management and performance challenges facing the FLRA in FY 2026. These challenges include the ongoing challenges of (1) The Continued Impact on the FLRA's Office of the General Counsel's Ability to Fulfill Its Mission Due to the Lack of a Confirmed General Counsel, and (2) Meeting Cybersecurity Requirements in a Resource-Constrained Environment, challenges we reported last year. Additionally, we identified one new challenge: (3) Ensuring Current and Effective Policies and Procedures. The FLRA has taken sufficient action to effectively mitigate the challenge of Achieving Performance Goals with Insufficient Funding that we reported in the FY 2024 PAR statement.

Our analysis considers the accomplishments the FLRA reported as of August 29, 2025. We noted progress that FLRA has made on (1) The Continued Impact on the FLRA's Office of the General

[1] Pub. L. No. 106-531, § 3 (codified at 31 U.S.C. § 3516).
[2] 31 U.S.C. § 3516(d).
[3] *Id.*
[4] *Id.*; *see also* Office of Management and Budget (OMB), OMB Circular A-136, *Financial Reporting Requirements*, § II.4.4. (July 14, 2025).

Counsel's Ability to Fulfill Its Mission Due to the Lack of a Confirmed General Counsel, and (2) Meeting Cybersecurity Requirements in a Resource-Constrained Environment.

The attached statement describes what we consider to be the most serious management and performance challenges facing the FLRA along with a brief assessment of management's progress in addressing them. We appreciate management's strong commitment to addressing these challenges and welcome comments to our assessment.

Attachment

Top Management and Performance Challenges for Fiscal Year 2026

Challenge 1: The Continued Impact on the FLRA's Office of the General Counsel's Ability to Fulfill Its Mission Due to the Lack of a Confirmed General Counsel

The Office of the General Counsel (OGC) plays a fundamental role in facilitating orderly, efficient, and effective change within the Federal Government. External challenges can make it difficult to achieve the overall mission. One significant management challenge is the eight-and-a-half-year vacancy in the position of General Counsel (GC), a role that is Presidentially-appointed and Senate-confirmed (PAS) (5 U.S.C. § 7104(f)(1)).[1]

This vacancy has impaired the FLRA's ability to achieve its mission because issuance of unfair-labor-practice (ULP) complaints are reserved exclusively to the GC's discretion (5 U.S.C. §§ 7104(f)(2)(B), 7118(a)(1)). Thus, if there is no GC or Acting GC, then the OGC cannot issue ULP complaints. As the GC position has been vacant since January 20, 2017, and there has been no Acting GC for most of that time, OGC's ability to perform its statutory duties has been severely impaired for over eight years.

This has had negative impacts on the efficiency and effectiveness of the Federal Government's labor-management relations system government-wide. ULP charges represent workplace conflicts. When OGC cannot act on the charges, workplace conflicts simmer and distract from agency missions. Moreover, the older the case, the more potential liability increases for the Federal Government in the form of higher backpay and interest.

The vacancy has also distorted OGC practices and created further delays that hurt the agencies, individuals, and bargaining unit representatives OGC serves. Parties file ULP charges that are investigated, but cannot be prosecuted in the absence of a PAS GC or Acting GC. Years pass and the number of ULP charge recommendations waiting for action grow. Then, during the limited tenure of an Acting GC, OGC must sprint to clear out those cases before the Acting GC's term expires, all while receiving new cases. The prioritization of the backlog cases caused delays in the resolution of other OGC cases.

[1] During this vacancy, Presidents have nominated individuals; the nominations expired without consideration by the full Senate. Nominations were made on: April 11, 2019; February 12, 2020; August 9, 2021; January 4, 2022; June 6, 2023; and January 8, 2024. The FLRA had Acting GCs for the periods January 20, 2017 to November 16, 2017, and March 23, 2021 to August 1, 2023.

Progress in Addressing this Challenge

As of the date of this statement, the GC position remains vacant. While this backlog may initially lessen with the implementation of Executive Order (EO) 14251, Exclusions from Federal Labor-Management Relations Programs (Mar. 27, 2025), and EO 14343, Further Exclusions from the Federal Labor-Management Relations Program (Aug. 28, 2025), the backlog will, nonetheless, continue to grow in the absence of a GC or Acting GC. FLRA stated that it continues to engage with key stakeholders to underscore the critical need for this position to be filled with a PAS GC.

The FLRA should continue to attempt to hasten the process of filling the GC vacancy by actively interacting with key decisionmakers and promptly addressing questions concerning nominees. The FLRA should continue these efforts in the coming year with the prospect that the vacancy may be filled in FY 2026.

References

- EO 14251, Exclusions from Federal Labor-Management Relations Programs, 90 Fed. Reg. 14553 (Mar. 27, 2025).
- EO 14343, Further Exclusions from the Federal Labor-Management Relations Program, 90 Fed. Reg. 42683 (Aug. 28, 2025).
- FLRA, Congressional Budget Justification for FY 2026 (May 30, 2025).
- The President, B-334563 (Comp. Gen. Feb. 8, 2023) ("Subject: *Violation of the Time Limit Imposed by the Federal Vacancies Reform Act of 1998: General Counsel, Federal Labor Relations Authority*").

Challenge 2: Meeting Cybersecurity Requirements in a Resource-Constrained Environment

FLRA is a small, independent agency facing ongoing challenges in maintaining a robust cybersecurity posture while operating with constrained budgets and limited staffing. The growing complexity and frequency of cyber threats, along with increasing regulatory requirements under the Federal Information Security Modernization Act of 2014 (FISMA)[2], make it difficult to keep pace with compliance expectations and operational demands. Despite progress in strengthening FLRA's information technology (IT) security, resource limitations continue to hinder the agency's ability to fully address the evolving landscape of cybersecurity risks.

In recent years, Federal cybersecurity requirements have expanded significantly. The annual FISMA review includes evaluating over 900 National Institute of Standards and Technology (NIST) controls, with agencies expected to meet stringent maturity levels across various domains, including risk management, incident response, and continuous monitoring.

The challenge lies in the disparity between the increasing cybersecurity demands and the limited funding and staffing available to small, independent agencies. While larger agencies have greater resources to address these challenges, smaller agencies often struggle to keep pace with the continuous flow of new requirements, guidance, and compliance mandates. This places additional pressure on the agency to meet government-wide cybersecurity standards without the necessary support to scale the agency's efforts.

Key Issues:

1. **Limited Resources:** As a small agency, the FLRA has limited funding and staffing to support comprehensive cybersecurity initiatives, which challenges the agency's ability to implement, monitor, and update the full range of security controls required by FISMA.
2. **Evolving Cyber Threats:** The cybersecurity landscape is dynamic, with threats becoming increasingly sophisticated and frequent. Keeping pace requires continuous investment in advanced tools, training, and expertise—resources that are often difficult to obtain due to budget constraints.
3. **Compliance and Maturity Levels:** Achieving a higher level of cybersecurity maturity, as mandated by FISMA, requires a holistic approach that encompasses risk management, continuous monitoring, and incident response.
4. **Competing Priorities:** The FLRA must balance cybersecurity requirements with other mission-critical priorities. Given finite resources, this often means making difficult decisions on funding allocation, which can lead to delays or reduced scope for cybersecurity initiatives.

[2] Pub. L. No. 113-283 (codified at 44 U.S.C. ch. 35).

Failing to address these challenges effectively can result in increased vulnerability to cyberattacks, potential data breaches, and reduced compliance with Federal security standards. Additionally, an ongoing FISMA finding related to cybersecurity may cause reputational harm, heightened oversight, and possible financial penalties.

Progress in Addressing this Challenge

The FLRA has made significant progress in advancing its IT security environment despite the resource constraints. In OIG's FISMA review for FY 2025, the findings supported closing 24 of the 25 recommendations from the prior year's review. Additionally, there were no new findings or recommendations. The one open recommendation for the FLRA relates to internal controls for supply chain risk management. In its response to the FISMA recommendation, FLRA noted its resource constraints, but committed to exploring options to address the recommendation, including possible support from other agencies.

Further, in OIG's FISMA review for FY 2025, OIG determined that the overall maturity level of the FLRA's information security program was "managed and measurable" (Level 4), *effective*. This was a critical improvement from the prior FY, when OIG determined the level to be "consistently implemented" (Level 3), *not effective*. FLRA attributed the improvement to FLRA employing a risk-based strategy and leveraging no-cost or cost-effective shared services provided by the Federal Government to address areas of highest risk.

Additionally, in FY 2025, OIG was able to close a recommendation from its privacy and data security review, related to the Incident Response Plan for breaches involving personally identifiable information, based on FLRA's having taking appropriate action to address the recommendation. Finally, the FLRA described in its Congressional Budget Justification for FY 2026 the IT capital improvements it will prioritize with any available resources.

References

- EO 14306, Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144, 90 Fed. Reg. 24723 (June 6, 2025).
- FLRA-OIG, *Evaluation of the FLRA's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2025*, Report No. MAR-25-09 (July 2025).
- FLRA-OIG, *Review of the Federal Labor Relations Authority's Privacy and Data Security Policies, Procedures, and Practices for Fiscal Year 2025*, Report No. MAR-25-06 (Apr. 2025).
- NIST, *NIST Cybersecurity Framework (CSF) 2.0* (Feb. 26, 2024).
- FLRA, Congressional Budget Justification for FY 2026 (May 30, 2025).

Challenge 3: Ensuring Current and Effective Policies and Procedures

Periodic review of agency policy and procedures is part of the standards of internal control in the Federal Government. These reviews serve as a crucial mechanism for identifying and addressing outdated or inadequate agency policies and are essential to enhancing internal controls utilized by management to fulfill the agency's objectives, mitigate risks in agency operations, and foster accountability. This process assists agencies in ensuring that their policies and procedures comply with current law and authoritative guidance, thereby effectively serving stakeholders such as the public, Congress, the President, and agency leadership.

Recent reviews by the OIG, conducted in FY 2024 with follow-up in FY 2025, identified various FLRA internal policies that were outdated or did not reflect current law or guidance. The OIG reviews found, in part:

- FLRA's Incident Response Policy and Standard Operating Procedure did not contain the necessary procedures for how to respond to personally identifiable information (PII) breaches and FLRA had no policy or procedures to minimize PII when testing, training, and research is conducted. FLRA addressed these findings and the OIG closed its recommendations in April 2025.
- Several FLRA policies contained nondisclosure provisions that ostensibly bound FLRA employees without inclusion of the requisite statutory language from the Whistleblower Protection Enhancement Act of 2012 (5 U.S.C. § 2302(b)(13)(A)). FLRA addressed this finding and OIG closed its recommendation in April 2025.
- FLRA policy *Protection of Personally Identifiable Information* was not current with relevant authorities. FLRA addressed the findings in that report and OIG closed its recommendations in July 2025.

FLRA promptly revised those policies OIG identified above. However, FLRA's policy about its policy system provides for a systematic and proactive approach: "A working group may be formed to: review existing FLRA policies; make recommendations regarding which policies should be updated and the timeline for doing so; and prepare proposals." FLRA Policy No. 1321, *Policy System*, § I (Sept. 7, 2018).

As of the date of this statement, the FLRA has several policies last updated in the 1980s, including its policies regarding reductions in force, workers compensation, and use of government telephone systems. While an older policy is not necessarily outdated, an older policy raises the question of whether relying on it is consistent with current law and government-wide policy.

The challenge of ensuring current and effective policies becomes especially pressing during periods of transition in Executive administration. With each new administration, there is an

immediate initiative to implement the administration's policy priorities through the Federal agencies. This has been the case in the current calendar year, and the FLRA must manage its limited resources to assess and revise outdated or inadequate policies to ensure their adherence to applicable law and authoritative guidance.

References

- FLRA-OIG, *Review of the Federal Labor Relations Authority's Privacy and Data Security Policies, Procedures, and Practices for Fiscal Year 2025*, Report No. MAR-25-06 (Apr. 2025).
- FLRA-OIG, *Follow-Up and Close-Out of the Review of FLRA Nondisclosure Requirements and Whistleblowing Rights*, Report No. MAR-25-05 (Apr. 2025).
- FLRA-OIG, *Follow-Up on the Evaluation of the Federal Labor Relations Authority's Compliance with the Privacy Act Mandatory Annual Training Requirement for Fiscal Year 2023*, Report No. MAR-25-08 (July 2025).
- Government Accountability Office (GAO), GAO-25-107721, *Standards for Internal Control in the Federal Government* (May 2025).
- FLRA, FLRA Policy No. 1321, *Policy System* (Sept. 7, 2018).