Congress of the United States

Washington, DC 20515

May 1, 2025

The Honorable Marvin E. Kaplan
Chairman
National Labor Relations Board
1015 Half Street SE
Washington, DC 20570-0001

Dear Chairman Kaplan:

We write with an urgent request for information related to the disclosure by a National Labor Relations Board (NLRB) whistleblower that agency officials possibly affiliated with the Department of Government Efficiency (DOGE) may have illegally exfiltrated multiple gigabytes of sensitive data, including the personal information of Americans who reported unfair labor practices. We are deeply concerned that these actions may constitute violations of the Privacy Act of 1974, which can carry criminal penalties, and the Federal Information Security Modernization Act (FISMA), which requires agency heads to notify Congress of major data breaches.

The National Labor Relations Board (NLRB) is an independent agency tasked with enforcing this nation's labor laws, including those related to organizing and collective bargaining. Like other agencies, the NLRB leverages information technology systems to process sensitive data in support of its mission. One such system is the Next Generation Case Management System, known as NxGen, a case tracking system that processes claims of unfair labor practice and representation cases. Sensitive data processed by NxGen include individuals' names, addresses, health/medical information, dates of birth, Social Security numbers, and bank account information.[1]

In order to protect the sensitive data at the NLRB and other federal agencies from unauthorized disclosure, and to uphold Americans' privacy in the wake of the Watergate scandal, Congress passed the Privacy Act of 1974. Under the Privacy Act, federal agencies may not disclose records contained within a system of records to third parties without an individual's prior written consent, subject to certain exceptions. Additionally, the Privacy Act stipulates that agency officials who improperly disclose records "willfully" shall be guilty of a misdemeanor and subject to fines of up to $5,000.[2]

To complement the Privacy Act, Congress passed laws in subsequent years to bolster the federal government's management of electronic information, including the Federal Information Security Modernization Act (FISMA). As required by FISMA, the Office of Management and Budget (OMB) must define the term "major incident" such that federal agencies can comply with mandated reporting requirements. Under this definition, agencies who suffer a major incident must notify relevant Congressional committees within 7 days of the incident's occurrence. Compliance with FISMA is vital for promoting the cybersecurity of federal government information systems and, consequently, protecting Americans' privacy.[3]

In particular, OMB defines "major incident" as:

1. Any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people; or

[1] 89 FR 24869.
[2] 5 U.S.C. § 552a.
[3] 44 U.S.C. § 3554.

2. A breach that involves personally identifiable information (PII) that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people; or

3. Any unauthorized modification of, unauthorized deletion of, unauthorized exfiltration of, or unauthorized access to the PII of 100,000 or more people.[4]

On April 15th, Daniel Berulis, an NLRB technology official, revealed through a whistleblower disclosure that staffers possibly affiliated with the Department of Government Efficiency (DOGE) may have exfiltrated multiple gigabytes of sensitive data from the NxGen system. A damning screenshot taken by Berulis of a graph tracking outbound traffic leaving NLRB's internal network shows a highly unusual spike on March 4th–shortly after DOGE staffers physically arrived at NLRB's headquarters. Not only was the spike inconsistent with NLRB's normal operations, but computer logs at the time of the spike were conspicuously missing from the system. According to Berulis, "nobody knows who deleted the logs or how they could have gone missing."[5]

Based on our understanding of the whistleblowers' disclosure, we are concerned that NLRB officials, especially those affiliated with DOGE, may have violated both the Privacy Act and FISMA.

With respect to the Privacy Act, it is overwhelmingly likely that one or more NLRB employees–and not foreign actors or criminals–perpetrated the massive data exfiltration on March 4th, violating the Act's disclosure requirements. Moreover, it appears that these officials did so without obtaining written consent nor receiving agency approval for an "exception" to the consent requirement, meaning they could be subject to criminal penalties.

And with respect to FISMA, it appears that the whistleblower discovered a "major incident" under any definition of the term proposed by OMB. NLRB subsequently failed to notify Congress, in apparent violation of its statutory requirements: as of writing, neither the House Oversight and Government Reform Committee nor House Education & the Workforce Committee have received notification with the required information about the incident. It is similarly alarming that NLRB failed to notify Congress even after conducting an internal investigation into the possible breach, demonstrating that you looked into the matter and either did not conclude a "major incident" occurred or failed to comply with FISMA's reporting requirements.

Congressional Democrats are committed to protecting Americans' privacy from abuse by foreign and domestic actors. To assist with our oversight responsibilities, we ask that you produce the following documents and respond to the following questions by May 16th, 2025:

1. All reports, communications, and written documentation produced during NLRB's investigation into Mr. Berulis's concerns that Tim Bearese, the NLRB's acting press secretary, confirmed took place in a statement to National Public Radio (NPR).

[4] Office of Management and Budget, Memorandum M-25-04, Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements (Jan. 2025).
[5] Jenna McLaughlin, "A whistleblower's disclosure details how DOGE may have taken sensitive labor data," NPR, April 15, 2025, https://www.npr.org/2025/04/15/nx-s1-5355896/doge-nlrb-elon-musk-spacex-security.

2. A signed attestation that NLRB determined the events which Mr. Berulis discovered qualify as a "major incident" under the definitions proposed by OMB or, alternatively, an explanation of why the NLRB will not make such a determination.

3. Why has the NLRB failed to notify relevant Congressional committees as required by FISMA, including the House Oversight and Government Reform and House Education & the Workforce Committees?

4. For each official who holds, or has previously held since January 20th, 2025, access to NLRB information technology systems:

    a. What is the nature of that employee's relationship with NLRB?

        i. If the employee is full-time, to what other agencies are they detailed?

        ii. If the employee is detailed to NLRB, from what agency are they detailed?

        iii. If the employee is a contractor, what firm do they work for?

    b. For each NLRB system that the employee previously had access to, currently has access to, or will have access to:

        i. What level of access to the system does the employee currently possess?

        ii. Who provided such access to the system?

        iii. What was the justification for providing such access to the system, especially if no other agency official had previously been granted the same level of access?

        iv. When was access to the system provided?

        v. What training, including security and privacy, were provided to the employee regarding their access to the system? Did this training take place before or after access was provided?

        vi. To the extent that access to the system was provided under a Privacy Act exception, what exception was invoked?

        vii. What security controls were implemented, if any, as a result of your granting the employee their access to the system?

        viii. Did the NLRB official who granted access to the system consider the cyber, operational, or privacy risks before doing so?

        ix. Has the employee modified, copied, shared, or removed any records from the system?

x. Has the employee modified the system in any way?

xi. Has the employee granted, revoked, or otherwise modified access to the system for any other users?

c. Can you commit to preserving all system logs related to access, development, and exfiltration consistent with the Federal Records Act?

d. Can you commit to otherwise documenting all critical decisions related to information technology systems at NLRB?

Thank you for your attention to this important matter. Should you have any questions, please do not hesitate to contact us or our staff.

Sincerely,

Lori Trahan
Member of Congress

Gerald E. Connolly
Member of Congress