SOCIAL SECURITY

Frank J. Bisignano, Commissioner

February 10, 2026

The Honorable Michael D. Crapo
Chairman, Committee on Finance
U.S. Senate
Washington, DC 20510

Dear Chairman Crapo:

I received your January 27, 2026 letter regarding Social Security Administration's (SSA) Notice of Corrections to the Record filed with the U.S. District Court for the District of Maryland on January 16, 2026.

Protecting personally identifiable information is a top priority at SSA.

Enclosed are SSA's responses to the specific questions in your letter. I am sending a similar response to Ranking Member Wyden.

Sincerely,

Frank J. Bisignano

Enclosures

1. The disclosure suggests that the SSA's policies for granting access to PII were not consistently followed during the time covered by the latest court filing. Based on this information, what steps has the agency taken, or does the agency plan to take, to ensure strict compliance with its policies regarding collecting, handling, and accessing PII going forward?

   Social Security Administration's current leadership took significant steps to improve its governance model from previous leadership. Personnel and organizational changes designed to enhance controls, security, service, and deliver better outcomes took place within weeks of the Commissioner being sworn into office on May 7, 2025.

   The following month, in June 2025, SSA's new organizational design was rolled out and the former Acting Commissioner, the Acting Chief Information Officer (who signed the data sharing agreement with an outside group and the subject of the January 2026 Notice of Corrections and Hatch Act referral), and Special Government Employees (SGEs) in the CIO office were separated.[1]

   Further, in its June 2025 reorganization, the agency placed its control environment as a tier one priority with the establishment of a Chief Risk Officer and a Chief of Security and Resiliency, both reporting to the Commissioner[2].

   The Chief Risk Officer leads a team focused on program integrity, fraud, improper payments, and quality of SSA decisions. The Chief of Security and Resiliency directs cybersecurity, physical security, SSA's Insider Threat Program, Security Clearance Program, Continuity of Operations, and the Security and Emergency Operations Center.

   On **control environment**, there are enhanced controls across the board leading to better oversight of issues and issue resolution. The agency employs a rigorous weekly protocol to resolve open audit issues with the Commissioner, and a daily meeting on cybersecurity, both with the purpose of achieving better outcomes.

   Since May 1, 2025, the agency closed audit recommendations totaling $13.8 billion in potential savings. The number of open audit recommendations is down from 180 in May to 105 today, a 42% reduction. The average age of an audit recommendation is now 1.32 years old versus 2.03 in May, a 35% reduction. The agency is currently at a 30-year low on open audit items.

   Additionally, each year, the agency undergoes several annual and targeted reviews of our programs, including the cybersecurity program.

---

[1] The former Acting Commissioner was placed on administrative leave on June 3, 2025, and is no longer employed by SSA. The former Acting CIO separated from SSA on June 18, 2025.

[2] Current and former SSA organizational charts are attached as Exhibit A. While the SSA reorganization was officially announced on September 3rd, SSA's top line organization was operating from June onward and as additional SES/Chiefs were appointed and onboarded into their roles. The Deputy Commissioner, Arjun Mody, assumed office on January 5, 2026.

Regarding cybersecurity, the Inspector General performs an annual review of the agency's compliance with the Federal Information Security Modernization Act (FISMA) Act. The agency has prioritized closing out prior years' audit recommendations and is on track to improve to a level four rating, on a one-to-five scale, which would be the highest in the agency's history. In addition to FISMA, the agency undergoes an annual Financial Statement Audit which tests information systems, an annual Inspector General review which reviews information systems and cybersecurity processes, GAO routine and random audits and reviews of information technology, and an annual agency internal review of cybersecurity controls.

On **cybersecurity controls**, the agency deploys encryption for data at rest and in transit, strict access controls, and secure data sharing through formal agreements and approved channels. In continuously monitoring the agency's systems, the following is a snapshot of the agency's cybersecurity control environment:

- Always-on, geographically dispersed cybersecurity operations center
- Authorization to Operate process (security controls are assessed and gaps identified prior to any information being used. Deficient controls are tracked and monitored with Plans of Actions and Milestones (POAM))
- Processes that follow guidelines from the National Institute of Standards and Technology's (NIST) Risk Management Framework (RMF)
- Techniques and tools used to protect networks and servers from attacks
- Firewalls and intrusion detection/prevention systems
- Multiple endpoint protection and anti-malware solutions to mitigate threats
- Logging and monitoring of system activity; user behavior analytics
- Forced USB device encryption, rules to alert and flag transmission of PII and sensitive data
- Security gates to prevent vulnerable code or code using vulnerable frameworks from being deployed
- Physical security controls for data centers and offices

The Insider Threat component of Security and Resiliency has additional controls in close collaboration with our cybersecurity program, including monitoring:

- Emails with attachments over a specific size
- Emails or documents containing keywords such as (CUI, FOUO, SENSITIVE, PROPRIETARY etc.)
- Webmail and Google drive docs
- Emails to domains on the DOW banned list
- Emails being sent from removable media
- Identifying and reviewing repeated emails (when an email is blocked and secondary attempts occur, or when it is going to public domains, i.e. Gmail, Outlook, etc.)
- Web uploads of large data files

- Monitoring is in place to detect and prevent unauthorized access, malware downloads, and data exfiltration attempts

Collectively, these measures are designed to safeguard sensitive data and ensure only authorized individuals and partners have access.

On **compliance**, SSA has established and continuously updates data protection policies and procedures that align with federal regulations. Employees are required to review and formally acknowledge these policies through signed documentation during onboarding and at designated intervals throughout their employment. SSA employees and contractors must also go through a suitability process, consistent with government-wide requirements followed by all federal agencies[3].

Further, SSA mandates completion of Information Security Awareness Training (ISAT) and privacy awareness training for all staff on an annual basis. This training covers proper data handling, recognizing and reporting potential security incidents, and understanding the importance of safeguarding sensitive information. Targeted training and testing occur at dedicated internals throughout the year to educate SSA employees on the evolving cybersecurity environment.

2. According to the latest disclosure, a member of the then-SSA DOGE Team was able to independently execute a data sharing agreement with an outside organization, seemingly without the knowledge of other agency employees or agency leadership. Following this discovery:

    a. What steps has SSA taken, or does SSA plan to take, to determine what, if any, data was improperly accessed or shared with the outside organization?

    The agency has conducted an exhaustive electronic stored information (ESI) search, a manual review by cybersecurity experts of all emails by SGEs over the past year and completed forensic imaging of hardware used by referenced individuals. There is no evidence that data was shared with the referenced outside organization.

    The actions described in the January 2026 Notice of Corrections have been referred to the Office of Special Counsel under the Hatch Act.

    b. What is SSA's current understanding of what, if any, data was shared with an outside organization?

    Following an exhaustive review across the agency, there is no evidence that data was shared with the referenced outside organization.

[3] All SGE hires were subject to the SSA suitability process in accordance with government-wide standards.

c. What steps has SSA taken, or does SSA plan to take, to prevent a similar situation arising in the future?

Social Security Administration's current leadership and governance model is delivering a control environment that provides for better outcomes. Rigorous audit reviews that integrate the Commissioner and Chiefs are delivering improved scores from auditors, agency savings, and bringing the agency current on the age of open audit items. The agency separated personnel and made structural changes to prioritize agency controls. This was all done within weeks of the new Commissioner assuming office. The agency is organized and has the tools to deliver on its control agenda for the American people.

3. Since early 2025, SSA has engaged in multiple information collection efforts in response to requests from Congress and the courts, yet new information appears to have just come to light in late 2025. What steps is the SSA taking to ensure the agency will be able to identify all information needed to fully address Congressional inquiries going forward?

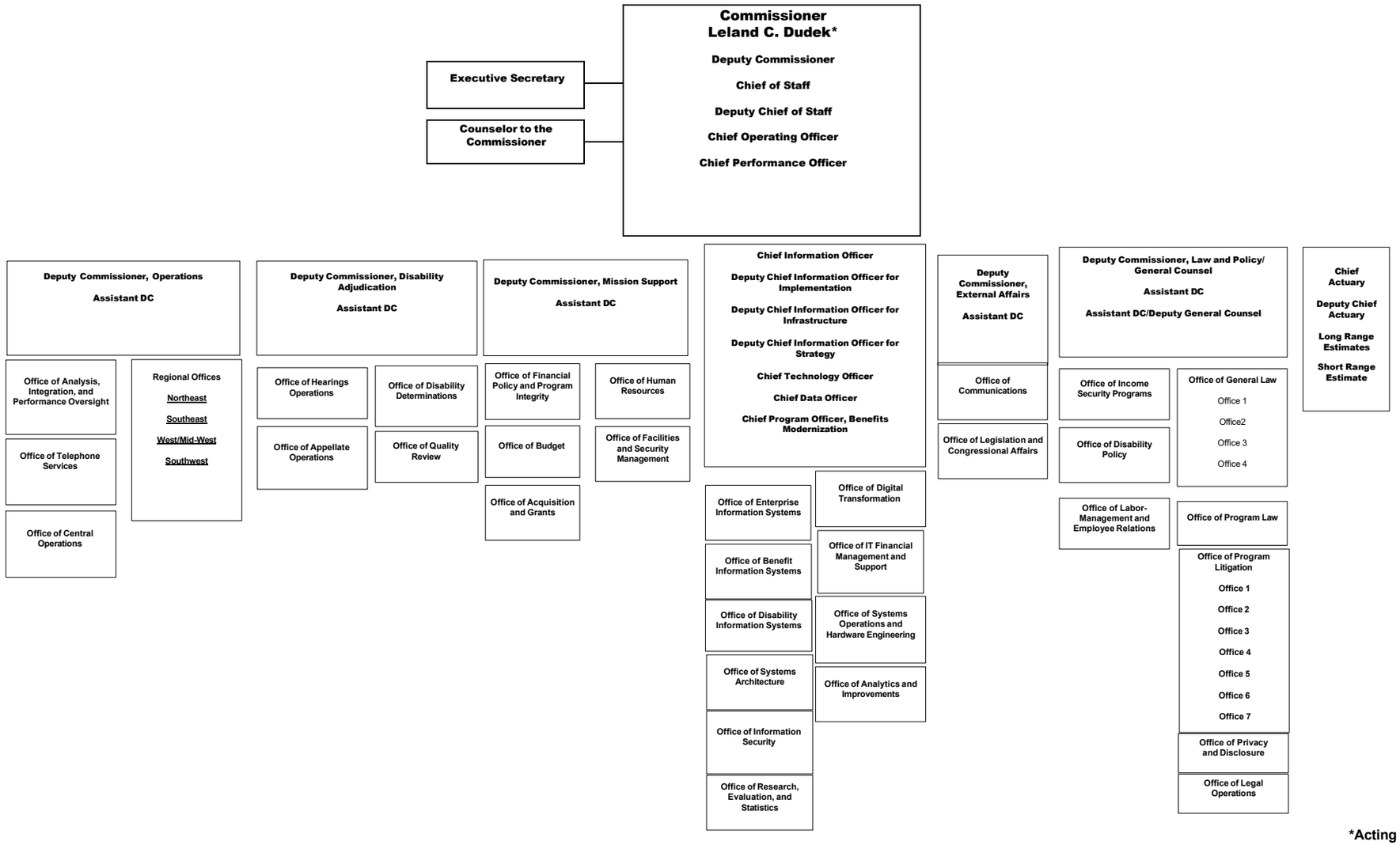
Social Security Administration has done an extensive electronic, manual, and forensic review of applicable emails, data transfers, and hardware of SGE personnel. In connection with various document collections and reviews in relation to litigation and audits, the agency identified the items that were the subject of the January 2026 Notice of Corrections. No additional information has been identified by the agency for Congress or the courts.

The early 2025 declaration was made by the Acting Commissioner, who was placed on administrative leave on June 3 and is no longer employed by the agency.

Exhibit A – Previous Organizational Chart

April 29, 2025

SOCIAL SECURITY ADMINISTRATION



*Acting

Exhibit A – Current Organizational Chart

June 2025

Social Security Administration