SOCIAL SECURITY
Frank J. Bisignano, Commissioner

September 16, 2025

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

Dear Chairman Crapo:

I am writing in response to your September 10, 2025 letter on data security at the Social Security Administration (SSA). I have been protecting personally identifiable information (PII) my entire career, and it has been and will continue to be my highest priority here at SSA. I appreciate the opportunity to address the concerns raised.

I can confirm, based on the agency's thorough review, that neither the Numident database nor any of its data has been accessed, leaked, hacked, or shared in any unauthorized fashion. SSA continuously monitors its systems for any signs of unauthorized access or data compromise, and we have not detected any such incidents involving the Numident database.

Please find enclosed the responses to your questions. I look forward to working with you and all Committee members to ensure the continued success of SSA.

Sincerely,

Frank J. Bisignano

Enclosure

1. **What actions did SSA take upon receipt of Mr. Borges' concerns about the agency's data security practices, including its handling of the Numident database and the data it contains?**

   After Mr. Borges first raised his concerns to relevant executives in his component on August 6, 2025, SSA designated two executives to interview him to further explore the nature of his concerns. Thereafter, the agency gathered key staff including the Acting Chief Information Security Officer (CISO), Chief Information Officers, and Chief Legal Counsel to review the allegation and information. The Acting CISO assessed the allegation that Numident data was stored in an unsecured cloud environment and determined it was unfounded. The location referred to in the whistleblower allegation is actually a secured server in the agency's cloud infrastructure which historically has housed this data and is continuously monitored and overseen—SSA's standard practice. SSA adhered to the defined agency data security practices which includes following National Institute Standards and Technologies (NIST) and Federal Information Security Modernization Act (FISMA) guidelines.

2. **What security measures and/or oversight mechanisms are in place at SSA to ensure sensitive data and PII are handled in accordance with applicable laws and regulations?**

   SSA adheres to FISMA, a law requiring federal agencies to implement security programs to protect their information systems. In essence, FISMA mandates that agencies adopt standards established by NIST to protect federal information.

   SSA's Security Assessment and Authorization Process applies the seven (7) distinct steps of the Risk Management Framework, as explained in NIST SP 800-37, Rev. 2 – "Risk Management Framework for Information Systems and Organizations: A System Lifecycle Approach for Security and Privacy."

   - Prepare
   - Categorization of Information and Information Systems
   - Select Security Controls
   - Implement Security Controls
   - Assess Security Controls
   - Authorize Information Systems
   - Continuous Monitoring

   The above process applies to all information systems including but not limited to those containing PII, specifically Numident, and all environments (secure cloud, data centers). Every information system goes through a privacy impact and risk assessment. SSA has a security operations center which monitors 24/7 for any threats or vulnerabilities impacting its networks.

3. **When did SSA first store PII in a cloud environment? Why and when did SSA select Amazon Web Services (AWS) to be the agency's cloud service provider?**

   SSA started to store PII in the agency's secure AWS cloud environment in late 2015/early 2016. SSA followed all competitive federal procurement requirements to select AWS as the agency's cloud service provider. AWS is a Federal Risk and Authorization Management Program (FedRAMP) cloud provider and offered the most attractive option for cloud services. At the time of selection, they were the industry leader and had been in the cloud infrastructure market for over 9 years.

4. **How did the SSA assess the risk of providing certain agency employees with the ability to transfer data from the Numident database to a private cloud within SSA's AWS cloud environment? Did this process diverge from the agency's usual risk assessment process? If so, how?**

   All employees are required to go through a vetting process prior to being granted access to SSA information systems. Based on their job functions, employees are granted the appropriate permissions to perform their work. Access to resources within the AWS environment is governed by the agency's established Systems Access Management protocols.

   The process did not diverge from standard agency processes.

   SSA never transferred the Numident database to a private cloud server within SSA's AWS cloud. SSA does not have a private cloud within its secure AWS.

5. **If there are any other matters relevant to the Committee better understanding the agency's data security practices generally or Mr. Borges' concerns specifically, please provide additional details for the Committee's awareness.**

   The agency's cybersecurity program is maintained by a team of over 300 dedicated security professionals. This expert team is responsible for designing, monitoring, and ensuring adherence to comprehensive security controls and policies across all information systems. Through their collective expertise and commitment, SSA proactively safeguards its digital assets, supports compliance with federal standards, and continuously enhances its security posture to address emerging threats.

   Standard access to systems resources containing PII requires users to complete an authorization request, which is subject to a tiered authorization process that includes a minimum of three approvers. This ensures that only individuals with appropriate clearance

and a demonstrated need-to-know are granted access, in accordance with agency policies and applicable federal regulations.

Prior to Mr. Borges originally raising his concerns to relevant executives in his component on August 6, 2025, he did not communicate with his peers in the security, data, and infrastructure groups who have oversight over these issues. Accordingly, they were not aware of the substance of his concerns. Although SSA was confident in the security of agency data and systems, SSA took Mr. Borges' concerns seriously and conducted a review.

The agency undergoes numerous IT security audits that provide insight into potential security gaps. Findings from these audits are integrated into SSA's continuous monitoring program, enabling the agency to promptly address vulnerabilities, strengthen its security posture, and ensure ongoing compliance with federal standards.

SSA's AWS cloud environment is audited yearly to ensure these controls are implemented and maintained.