Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

Audit Summary

Digital Identity in my Social Security

142307 September 2023

Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

MEMORANDUM

Date: September 26, 2023 **Refer to:** 142307

To: Kilolo Kijakazi
Acting Commissioner

From: Gail S. Ennis
Inspector General

Subject: Digital Identity in my Social Security

The attached final report summarizes the results of our review. The objective was to determine whether the Social Security Administration's identity verification controls for the *my* Social Security portal were compliant with Federal requirements.

Our audit report (A-14-18-50486) results contain information that, if not protected, could result in adverse effects to the Agency's information systems. In accordance with government auditing standards, we have separately transmitted to SSA management our audit's detailed findings and recommendations and excluded from this summary certain sensitive information because of the potential damage if the information is misused. We determined the omitted information neither distorts the audit results described in this report nor conceals improper or illegal practices.

If you wish to discuss the final report, please call me or have your staff contact Michelle L. Anderson, Assistant Inspector General for Audit.

Attachment

Digital Identity in my Social Security 142307

September 2023 **Results in Brief**

Objective

To determine whether the Social Security Administration's (SSA) identity verification controls for the *my* Social Security portal were compliant with Federal requirements.

Background

In May 2012, SSA introduced the *my* Social Security Internet-services portal. Since then, it has helped to reduce traffic in field offices and calls to its National 800-number Telephone Service. Through their *my* Social Security accounts, private citizens may view their Social Security records or conduct services online.

In June 2017, the National Institute of Standards and Technology (NIST) issued guidance that sets the baseline requirements for digital identity services and addresses risks associated with authentication and identify-proofing errors. The guidance also provides technical requirements for identity proofing and authenticating users who are interacting with Federal information technology systems, such as Login.gov. In May 2019, the Office of Management and Budget required that Federal agencies implement the NIST guidance and any successive versions as the foundation for digital identity.

We reviewed Federal requirements and SSA policies, procedures, and internal control documentation. We also interviewed Agency personnel responsible for the digital identity controls.

Results

SSA's identity verification controls for the *my* Social Security portal were not fully compliant with Federal requirements. The online services provide a valuable resource for individuals to conduct business with SSA by without having to visit a local field office or call the National 800-Number Telephone System. As SSA adds more services behind the *my* Social Security portal, it will become even more important that SSA safeguard the information and ensure only the correct individual can access the information. SSA's identity-proofing process creates a risk that someone could claim an incorrect identity.

Recommendations

We made three recommendations to help ensure SSA implements stronger digital identity controls that are compliant with Federal requirements for the public to access *my* Social Security online services.

Recommendations

SSA agreed with our recommendations.

TABLE OF CONTENTS

ABBREVIATIONS

Fed. Reg.	Federal Regulation
GAO	Government Accountability Office
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	Office of Management and Budget
SSA	Social Security Administration

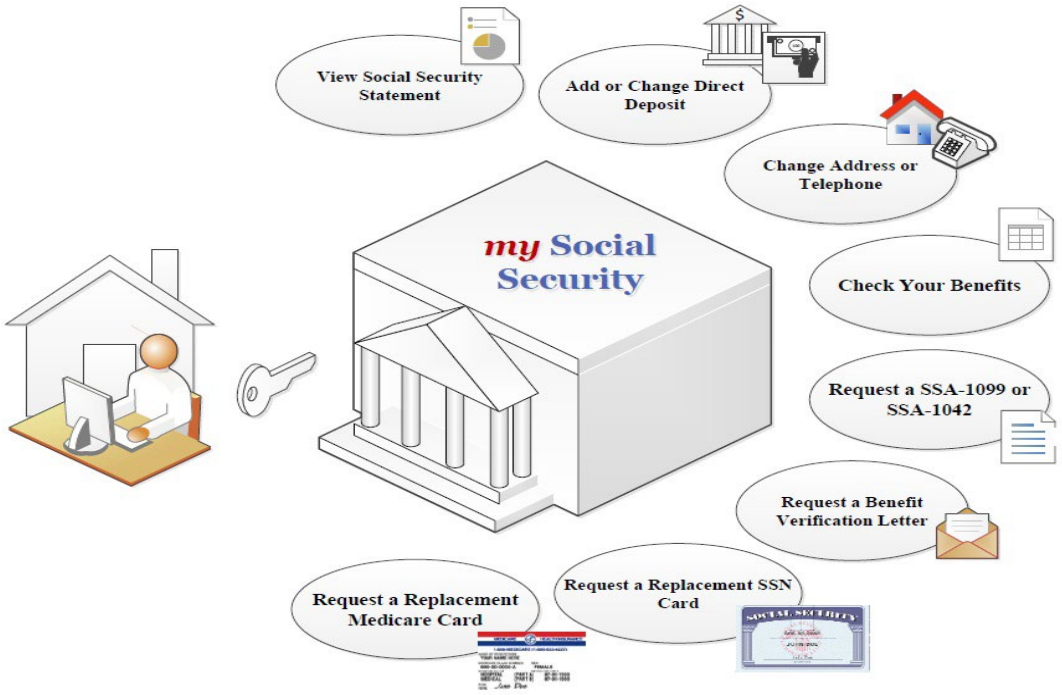
OBJECTIVE

Our objective was to determine whether the Social Security Administration's (SSA) identity verification controls for the *my* Social Security portal are compliant with Federal digital identity requirements.

BACKGROUND

In May 2012, SSA introduced the *my* Social Security Internet-services portal. Since then, SSA moved more services behind *my* Social Security. These online services have helped to reduce traffic in field offices and calls to its National 800-number Telephone Service. Through their *my* Social Security account, private citizens may view their Social Security records or conduct a range of services online, including: changing an address or direct-deposit information, requesting a replacement Social Security number or Medicare card, checking the status of benefit applications, verifying earnings, accessing Social Security statements, and obtaining benefit verification letters (see Figure 1). As of December 2022, over 76 million individuals had established *my* Social Security accounts. See Appendix A for what the services an individual can access through the online portal.

Figure 1: SSA's *my* Social Security



my Social Security Accounts

In May 2021, SSA began partnering with the General Services Administration's Login.gov to allow customers to access *my* Social Security.[1] Customers may have previously created accounts with Login.gov or will be able to create new accounts. When customers access SSA's Website, they must choose to sign in with SSA-provided *my* Social Security credentials,[2] Login.gov credentials, or credentials provided by a commercial third party.[3] If customers choose to sign in with Login.gov credentials, they are directed to Login.gov to provide one factor – their usernames and passwords, and a second factor.

New registrants are prompted to create Login.gov credentials or sign in with existing credentials to access their *my* Social Security accounts. After the customer successfully signs in, they are redirected to, and must accept, the *my* Social Security Terms of Service screen to proceed with the online registration process. According to SSA policy, a user begins identity proofing when the individual accepts the Terms of Service and ends when SSA verifies the individual. Once a user establishes and signs in to a *my* Social Security account, they may immediately access a significant amount of sensitive information.

Digital Identity Federal Guidelines

Public-facing systems that allow users to access personally identifiable information or to alter customer data are particularly vulnerable to fraudulent activity. Executive Order 13681 directs the development of whole-of Government guidance that requires that agencies employ an effective identity proofing process, as appropriate, when personal information is released.[4] Identity proofing establishes whether users are who they claim to be. Authentication establishes that a user who attempts to access a digital service is in control of one or more valid authenticators associated with that subject's digital identity.[5] Additionally, for services in which return visits are applicable, successfully authenticating provides reasonable assurance the subject accessing the service is the same as the subject who accessed it previously.

---

[1] Login.gov was a General Services Administration project that sought to develop secure, user-friendly ways for the public to access Government Websites. Login.gov provides a simple, secure, and private way for the public to access Government Websites. With one account and password, users can securely sign in to participating Government Websites and securely verify their identity.

[2] Until May 2021, customers created usernames and passwords directly with SSA.

[3] In July 2023, SSA announced plans to retire legacy SSA credentials. Once completed, users who have legacy credentials will be required to transition their account to credentials from Login.gov or a commercial third party. At the conclusion of this transition process, all users will be required to sign in using one of the third-party credentials.

[4] *Improving the Security of Consumer Financial Transactions*, Executive Order No. 13681, 79 Fed. Reg. 63489 (October 23, 2014).

[5] NIST, *Digital Identity Guidelines*, *800-63-3*, p. iv (June 2017, amended March 2020).

In June 2017, the National Institute of Standards and Technology (NIST) issued guidance which sets the baseline requirements for digital identity services and addresses risks associated with authentication and identify proofing errors.[6] The guidance also provides technical requirements[7] for identity proofing and authenticating users who are interacting with government information technology systems, such as Login.gov.[8] In May 2019, the Office of Management and Budget (OMB) required Federal agencies implement the NIST guidance and any successive versions.[9]

Digital Identity Risk Management

Agencies are required to assess the risk of identity proofing and authentication errors separately to determine the required assurance level for each type of transaction.[10] Risk assessments determine the extent to which risk must be mitigated by the identity proofing and authentication processes.[11] After evaluating the potential risks associated with an information system, the Agency should select assurance levels for identity proofing and authentication and determine the processes and technologies it will employ to meet each assurance level.

NIST requires a two-component, risk-based process: Identity Assurance Level for identity proofing and Authenticator Assurance Level for authentication.[12] The NIST framework for each provides three levels of risk mitigation that agencies may select. For both Levels an agency chooses an option based on its risk profile, the potential harm "caused by an attacker making a successful false claim of an identity" and the potential harm "caused by an attacker taking control of an authenticator[13] and accessing the agency['s] systems", respectively.[14] Additionally, when agencies' public-facing systems provide access to Federal tax information, such as earnings records available through *my* Social Security, the Internal Revenue Service requires that agencies implement Identity Assurance Level 2 and use Authenticator Assurance Level 2.[15]

---

[6] NIST, *Digital Identity Guidelines, 800-63-3* (June 2017, amended March 2020); *Digital Identity Guidelines, Enrollment and Identity Proofing, 800-63A* (June 2017, amended March 2020); *Digital Identity Guidelines, Authentication and Lifecycle Management, 800-63B* (June 2017, amended March 2020).

[7] NIST distinguishes between "normative" material that is mandatory and "informative" material that provides guidance but does not present mandatory requirements. NIST, *Digital Identity Guidelines*, *800-63-3*, p. v (June 2017, amended March 2020).

[8] NIST, *Digital Identity Guidelines*, *800-63-3*, p. iii (June 2017, amended March 2020).

[9] OMB, *Enabling Mission Delivery Through Improved Identity, Credential, and Access Management, M-19-17* (2019).

[10] NIST, *Digital Identity Guidelines*, *800-63-3*, ch. 5.1, p. 17 (June 2017, amended March 2020).

[11] NIST, *Digital Identity Guidelines*, *800-63-3*, ch. 5.1, p. 17 (June 2017, amended March 2020).

[12] Refer to Appendix B for more information regarding Assurance Levels.

[13] The claimant possesses and controls an authenticator (typically a password) that is used to authenticate the claimant's identity. NIST, *Digital Identity Guidelines*, *800-63-3*, p. 42 (June 2017, amended March 2020).

[14] NIST, *Digital Identity Guidelines*, *800-63-3*, p. vi (June 2017, amended March 2020).

[15] Internal Revenue Service, Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies*, ch. 3.3.8.c, p. 86 (November 2021).

SSA conducted risk assessments for the transactions in *my* Social Security and determined the transactions required Identity Assurance Level 2 and Authenticator Assurance Level 2. To achieve Identity Assurance Level 2, SSA must obtain, validate, and verify users' identity documentation.[16] To achieve Authenticator Assurance Level 2, SSA must ensure users can prove possession and control of two distinct authentication factors (such as a password and an identification badge) or through a defined sequence of messages with users (such as entering a code sent to a mobile device into a Web authentication session). Additionally, NIST requires approved cryptographic techniques at Authenticator Assurance Level 2.[17]

Scope and Methodology

To achieve our objective, we reviewed Federal requirements and SSA policies, procedures, and internal control documentation. We also interviewed Agency personnel responsible for the digital identity controls. See Appendix C for additional information about our scope and methodology.

RESULTS OF REVIEW

SSA's identity verification controls for the *my* Social Security portal did not fully comply with Federal requirements. [18, 19]

Identity Proofing

According to NIST, identity proofing establishes that a subject is who they claim to be. Digital authentication establishes that a subject attempting to access a digital service is in control of one or more valid authenticators associated with that subject's digital identity.[20] Agencies complete identity proofing in 3 steps:

1. **Resolution.** Core attributes and evidence are collected. This step uniquely distinguishes an individual within a given population or context.[21] Agencies may use knowledge-based

---

[16] NIST, *Digital Identity Guidelines: Enrollment and Identity Proofing*, *800-63A*, ch. 4.4, pp. 8 through11 (June 2017, amended March 2020).

[17] NIST, *Digital Identity Guidelines: Authentication and Lifecycle Management*, *800-63B*, ch. 4.2, pp. 6 through8 (June 2017, amended March 2020).

[18] Our audit report contains information that, if not protected, could result in adverse effects to the Agency's information systems. In accordance with government auditing standards, we have separately transmitted to SSA management our audit report, which details our findings and recommendations. We excluded from this summary certain sensitive information because of the potential damage if the information is misused. We have determined the omitted information neither distorts the audit results described in this report nor conceals improper or illegal practices.

[19] We found similar issues in our review, *Access to the Social Security Administration's my Social Security Online Services* (Limited Distribution) *A-14-15-15010* (September 2016). For a list of all prior audits on *my* Social Security, see Appendix D.

[20] NIST, *Digital Identity Guidelines*, *800-63-3*, p. iv (June 2017, amended March 2020).

[21] NIST, *Digital Identity Guidelines: Enrollment and Identity Proofing*, *800-63A*, ch. 5.1, p. 15 (June 2017, amended March 2020).

verification for added confidence; however, to achieve Identity Assurance Level 2, agencies must collect additional identity evidence.[22]

2. **Validation**. Evidence is validated to determine the identity information's authenticity, validity, and accuracy and ensure the claimed identity exists in the real world.[23] To achieve Identity Assurance Level 2, agencies must validate each piece of evidence with a process that can achieve the same strength as the evidence presented.[24] (Refer to Appendix E for more information regarding strengths of identity evidence.)
3. **Verification.** Evidence is verified to confirm the claimed identity is associated with the real person supplying the evidence.[25]

We reviewed SSA's identity evidence resolution, validation, and verification process and found deficiencies.

Identity Proofing for Standard my Social Security Accounts

To establish a standard *my* Social Security account, a user must provide some basic identifying information.[26] SSA verifies the information agrees with SSA's internal records or to an external data source through a vendor.

Although SSA determined *my* Social Security requires Identity Assurance Level 2, it does not collect identity evidence for all new account registrations. The Agency verification of personal information provided, in combination with demonstrated control of a known address, meets the "identity evidence" NIST requires. However, presentation of identity evidence, such as a driver's license, is required at Identity Assurance Level 2.

"Extra Security" Accounts

Customers can choose to establish accounts with more security than a standard account. SSA refers to these as "extra security" accounts. However, for *my* Social Security, there is no difference between what most users can access using standard or "extra security" accounts.[27]

---

[22] Because of the wide availability of knowledge-based personal information, knowledge-based verification presents limited strength to the verification process. NIST, *Conformance Criteria for NIST 800-63A Enrollment and Identity Proofing and NIST 800-63B, Authentication and Lifecycle Management*, Appendix A, p. 63 (June 2020); NIST, *Digital Identity Guidelines: Enrollment and Identity Proofing*, *800-63A*, chs. 4.4.1.1 and 4.4.1.2, p. 9 (June 2017, amended March 2020).

[23] NIST, *Digital Identity Guidelines: Enrollment and Identity Proofing*, *800-63A*, ch. 5.2 p. 15 (June 2017, amended March 2020).

[24] NIST, *Digital Identity Guidelines: Enrollment and Identity Proofing*, *800-63A*, ch. 4.4.1.3, p. 9 (June 2017, amended March 2020).

[25] NIST, *Digital Identity Guidelines: Enrollment and Identity Proofing*, *800-63A*, ch. 5.3, p. 19 (June 2017, amended March 2020).

[26] The customer must ensure formatting entries are corrected. The customer may also correct formatting entries with no limitations on the number of corrections.

[27] SSA does require "extra security" accounts for users to access such *my* Social Security services as the wage reporting tool in Business Services Online or submitting medical evidence through Electronic Records Express.

Although SSA requests identity evidence for "extra security" accounts, users can manually enter the requested information or upload a photograph of the state-issued identification. If customers do not have state-issued identification, they can answer out-of-wallet questions. Evidence SSA requests does not support the Identity Assurance Level 2 requirements.

Additionally, users do not need the "extra security" account to access the personal information in *my* Social Security. The Agency may mislead users into thinking that subjecting themselves to the "extra security" process is somehow improving the security of their accounts.
We reviewed SSA's identity evidence collection, validation, and verification process for "extra security" accounts and found the "extra security" accounts do not meet Identity Assurance Level 2 requirements. Therefore, the Agency may not achieve the level of assurance NIST and the Internal Revenue Service require.

Login.gov Procedures

Customers who choose to log into *my* Social Security using Login.gov credentials are directed to Login.gov's Website to provide their registration information. Customers who have verified their identities with Login.gov do not need to re-verify their identities with SSA and will proceed to *my* Social Security accounts. However, the General Services Administration's Office of Inspector General found Login.gov ". . . has never met [NIST's] requirements for [Identity Assurance Level] 2."[28] SSA relies on Login.gov's assertion that users' identities have been verified.

Authentication for Existing *my* Social Security Accounts

We reviewed SSA's authentication process and found deficiencies for accounts created before September 2021. Therefore, for those accounts, the Agency may not achieve the level of assurance NIST and the Internal Revenue Service require. The Agency plans to remediate this issue beginning in Fiscal Year 2024.

Risk Assessments

Agencies are required to assess the risk of identity proofing and authentication errors separately to determine the required assurance level for each type of transaction. After evaluating the potential risks, agencies determine the degree to which they must be confident in the user's asserted identity.[29] We reviewed SSA's risk assessments for 31 transaction types in *my* Social Security and found deficiencies in SSA's risk assessment process.

CONCLUSION

The online services provide a valuable resource for individuals to conduct business with SSA by saving time and by not having to visit a local field office or call the National 800 Number Telephone System. As SSA adds more services behind the *my* Social Security portal, it will

[28] General Services Administration, OIG, *GSA Misled Customers on Login.gov's Compliance with Digital Identity Standards,* JE23-003 (Redacted), p. 6 (March 2023).

[29] NIST, *Digital Identity Guidelines*, *800-63-3*, ch. 5.1, p. 17 (June 2017, amended March 2020).

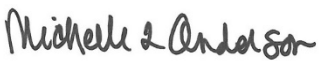
become even more important that SSA safeguard the information and ensure only the correct individual can access the information.

RECOMMENDATIONS

We made three recommendations to SSA to strengthen its digital identity controls and ensure it is fully compliant with all Federal requirements.

AGENCY COMMENTS

SSA agreed with our recommendations. Please see Appendix F for the text of the Agency's full response.



Michelle L. Anderson
Assistant Inspector General for Audit

APPENDICES

Appendix A – SERVICES AN INDIVIDUAL CAN ACCESS WITH A *MY* SOCIAL SECURITY ACCOUNT

The *my* Social Security program is a suite of online services available to most adult numberholders. It provides a single point of access to a variety of information and electronic services. Applicants access *my* Social Security using the Electronic Access/Registration of Most Everyone application, which offers a single credential (User ID) issuance, management, and authentication system that can be used by any individual seeking to conduct business online with the Social Security Administration (SSA). Below is a list of things an individual can do with a *my* Social Security account:

- Request a replacement Social Security card;
- Get personalized retirement benefit estimates;
- Get estimates for spouse's benefits;
- Get proof that you do not receive benefits;
- Check your application status;
- Get your *Social Security Statement*;
- Set up or change direct deposit;
- Get a Social Security 1099 (SSA-1099) form;
- Opt out of mailed notices for those available online;
- Print a benefit verification letter; and
- Change your address.

Appendix B – IDENTITY AND AUTHENTICATOR ASSURANCE LEVELS

The National Institute of Standards and Technology (NIST) has established identity and authenticator assurance levels.[1]

Identity Assurance Levels

The Identity Assurance Level is the robustness of the identity proofing process to confidently determine the individual's identity and is selected to mitigate potential identity-proofing errors. Each Identity Assurance Level describes the degree of confidence the user's claimed identity is their real identity.

- **Identity Assurance Level 1:** NIST does not require a link from the applicant to a specific real-life identity. Any attributes provided are self-asserted or should be treated as such.
- **Identity Assurance Level 2:** NIST requires verification that the applicant's real-world existence is supported, either remotely or in-person.
- **Identity Assurance Level 3:** NIST requires in-person identity proofing.[2]

Authenticator Assurance Levels

For services in which return visits are applicable, a successful authentication provides reasonable risk-based assurances the customer accessing the service today is the same as that which assessed the service previously. Authenticator Assurance Level is the robustness of the authentication process itself and the binding between something the applicant possesses and controls[3] and a specific individual's identifier. Authenticator Assurance Level is selected to mitigate potential authentication errors (that is, a false claimant using a credential that is not rightfully theirs).[4]

- **Authenticator Assurance Level 1:** Some assurance the claimant controls an authenticator. NIST requires either single- or multi-factor authentication.
- **Authenticator Assurance Level 2:** High confidence the claimant controls an authenticator. NIST requires proof of possession and control of two different authentication factors through a secure authentication protocol. Approved cryptographic techniques are also required.

---

[1] NIST, *Digital Identity Guidelines*, *800-63-3*, pp. iv through vii (June 2017, amended March 2020).

[2] NIST, *Digital Identity Guidelines, 800-63-3*, ch. 5.2, Table 5-1, p. 18 (June 2017, amended March 2020).

[3] The cornerstones of authentication are: (1) Something you know (such as a password); (2) Something you have (such as an identification badge or a cryptographic key); and (3) Something you are (such as a fingerprint or other biometric data). NIST, *Digital Identity Guidelines*, *800-63-3*, ch. 4.3.1, p 12 (June 2017, amended March 2020).

[4] Stronger authentication (a higher level) requires malicious actors to have better capabilities and expend greater resources to successfully subvert the authentication process. Authentication at higher levels can effectively reduce the risk of attacks. NIST, *Digital Identity Guidelines: Authentication and Lifecycle Management, 800-63B*, ch. 2, p. 2 (June 2017, amended March 2020).

- **Authenticator Assurance Level 3:** Very high confidence the claimant controls an authenticator. NIST requires a "hard" cryptographic authenticator that provides verifier impersonation resistance.[5]

[5] NIST, *Digital Identity Guidelines, 800-63-3*, ch. 5.2, table 5-2, p. 19 (June 2017, amended March 2020).

Appendix C – SCOPE AND METHODOLOGY

To accomplish our objectives, we:

- Reviewed National Institute of Standards and Technology (NIST) *Digital Identity Guidelines*; *Special Publication* 800-63; Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource* (June 2017, amended March 2020), (July 28, 2016); and OMB Memorandum M-19-17, *Enabling Mission Delivery Through Improved Identity, Credential, and Access Management* (May 21, 2019).
- Reviewed the authentication risk assessments for *my* Social Security applications to ensure the Social Security Administration (SSA) properly identified risks and assessed identity assurances at the appropriate level to protect personally identifiable information and Federal tax information.
- Reviewed SSA's identity-proofing/enrollment process for online services to determine whether SSA adequately addresses the potential risk of unauthorized release of personal information.
    - Reviewed recent enhancements to SSA's identity-proofing/enrollment process.
    - Reviewed SSA's plans for removing knowledge-based verification from the identity-proofing/enrollment process.
    - Reviewed the Credit Reporting Agency's role in the identity proofing/enrollment process.
- Determined whether SSA's multi-factor authentication process for online services addresses the potential risk of unauthorized access to sensitive information.
    - Determined whether SSA is using authenticators that meet the NIST requirements.
    - Determined whether SSA allowed the same email address or cellular telephone number to be used as the authenticator for multiple accounts.
- Verified whether applications have audit logs available for investigation if needed.
- Reviewed SSA's partnerships with third-party credential services.
- Reviewed SSA's future initiatives to improve the online authentication to access its online services.

We conducted our audit from December 2020 through June 2023. The principal entity reviewed was the Office of Information Security under the Office of the Deputy Commissioner for Systems.

We assessed the significance of internal controls necessary to satisfy the audit objective. This included an assessment of the five internal control components, including control environment, risk assessment, control activities, information and communication, and monitoring. In addition, we reviewed the principles of internal controls associated with the audit objective. We identified the following components and principles as significant to the audit objective.

- Component 2: Risk Assessment
  - Principle 7 - Identify, analyze, and respond to risk
  - Principle 8 - Assess fraud risk
- Component 3: Control Activities
  - Principle 10 - Design control activities
  - Principle 11 - Design activities for the information system
  - Principle 12 - Implement control activities
- Component 4: Information and Communication
  - Principle 13 – Use quality information
- Component 5: Monitoring
  - Principle 16 - Perform monitoring activities
  - Principle 17 - Remediate deficiencies

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix D – Related Office of the Inspector General Reports

The Social Security Administration (SSA), Office of the Inspector General has issued several reports related to *my* Social Security and online authentication as well as one recent report from the Government Accountability Office (GAO).

Table D–1: Related Reports

Report Title and Date Issued	Findings and Recommendations
Federal Agencies Need to Strengthen Online Identity Verification Processes (GAO-19-288), May 2019	SSA did not yet have specific plans and milestones to achieve its goal of implementing enhanced remote identity proofing processes by Fiscal Year 2020. SSA officials stated they cannot develop specific plans until they can identify an alternative method(s) that all members of the public with which the agency interacts can use successfully. GAO recommended the Commissioner of Social Security develop a plan with specific milestones to discontinue knowledge-based verification, such as using Login.gov or other alternative verification techniques.
Unauthorized my Social Security Direct Deposit Changes Through May 2018 (Limited Distribution) (A-01-18-50669), September 2019	An estimated $33.5 million in benefits for 20,878 beneficiaries was misdirected from January 2013 through May 2018 because of unauthorized direct deposit changes made through *my* Social Security. We also estimated that, from January 2013 through May 2018, SSA prevented $23.9 million in benefits from being misdirected from 19,662 beneficiaries whose direct deposit account was changed without their authorization. We did not make additional recommendations for corrective action because, as of June 2019, SSA had not implemented our recommendation from September 2016.
Unauthorized my Social Security Direct Deposit Changes in Calendar Years 2014 Through 2016 (Limited Distribution) (A-01-17-50210), August 2017	An estimated $10.9 million in benefit payments for about 7,200 beneficiaries was misdirected in Calendar Years 2014 through 2016. Comparing our analysis of the Calendar Year 2014 through 2016 data to our prior review of Calendar Year 2013 data showed the amount of benefits misdirected through *my* Social Security decreased. We also estimated SSA prevented about $14.1 million in benefits from being misrouted from about 11,900 beneficiaries whose direct deposit bank account was changed without their authorization. We made recommendations to SSA related to verifying the identities of *my* Social Security users in our September 2016 report. As a result, we did not make any additional recommendations.
Access to the Social Security Administration's my Social Security Online Services (Limited Distribution) (A-14-15-15010), September 2016	SSA initially concluded it needed some degree of confidence that *my* Social Security users are who they claim to be. However, in June 2016, SSA conducted a new risk assessment and concluded it needed a higher degree of confidence in users' asserted identities. We made two recommendations to strengthen controls over access to *my* Social Security. SSA agreed with both recommendations.

Report Title and Date Issued	Findings and Recommendations
Unauthorized Direct Deposit Changes through my Social Security (Limited Distribution) (A-01-14-24011), September 2015	Some beneficiaries' payments were delayed, and some faced dire financial need, requiring that they contact SSA for immediate assistance. We estimated about $20 million in benefit payments to approximately 12,200 beneficiaries was misdirected between January 2013 and January 2014. Additionally, we estimated that SSA prevented about $6 million in benefits from being misrouted for about 5,300 beneficiaries whose direct deposit bank account was changed without their authorization. SSA had strengthened its controls over my Social Security accounts to address potential fraud and improve service to beneficiaries.
The Social Security Administration's Authentication Risk Assessment for the Internet Social Security Number Replacement Card Project (Limited Distribution) (A-14-14-24130), May 2015	SSA's authentication risk assessment of the Social Security Number Replacement Card application required a high degree of confidence that online users were who they claimed to be. However, in accordance with Office of Management and Budget policy, the Agency opted to develop a Risk Mitigation Strategy and planned to implement the application with a lower level of confidence that users were who they claimed to be. Given the risks associated with this online application, we encouraged SSA to continue developing mitigating controls.
Direct Deposit Changes Initiated Through Financial Institutions and the Social Security Administration's Internet and Automated 800-Number Applications (Limited Distribution) (A-14-12-21271), December 2012	Financial institutions provided SSA with unauthorized direct deposit changes the Agency processed. Although SSA had some controls to prevent this, we identified weaknesses in SSA's authentication process. We made nine recommendations. SSA agreed with eight and disagreed with one.
The Social Security Administration's eAuthentication Process (A-14-11-11115), October 2011	SSA took steps to implement an electronic authentication process to create a secure authentication protocol for citizen-to-Government Internet applications at the level to establish some confidence in the validity of the asserted identity. We made six recommendations with which the Agency agreed.

Appendix E – STRENGTHS OF IDENTITY EVIDENCE

Table E–1 lists strengths, ranging from unacceptable to superior, of identity evidence that is collected to establish a valid identity.[1] Unless otherwise noted, to achieve a given strength the evidence shall, at a minimum, meet all the qualities listed.

Table E–2: Strengths and Qualities of Identity Evidence

Strength	Qualities of Identity Evidence
Unacceptable	No acceptable identity evidence provided.

Weak	• The issuing source of the evidence did not perform identity proofing.
	• The issuing process for the evidence means it can reasonably be assumed to have been delivered into the customer's possession.
	• The evidence contains:
	  ○ At least one reference number that uniquely identifies itself or the person to whom it relates, OR
	  ○ The issued identity evidence contains a photograph or biometric template (of any modality) of the person to whom it relates.

Fair	• The issuing source of the evidence confirmed the claimed identity through an identity-proofing process.
	• The issuing process for the evidence means it can reasonably be assumed to have been delivered into the possession of the person to whom it relates.
	• The evidence:
	  ○ Contains at least one reference number that uniquely identifies the person to whom it relates,
	  ○ Contains a photograph or biometric template (any modality) of the person to whom it relates, OR
	  ○ Can have ownership confirmed through knowledge based verification.
	• Where the evidence includes digital information, that information is protected using approved cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the claimed issuing source to be confirmed.
	• Where the evidence includes physical security features, it requires proprietary knowledge to be able to reproduce it.
	• The issued evidence is unexpired.

[1] NIST, *Digital Identity Guidelines: Enrollment and Identity Proofing Requirements*, 800-63A, ch. 5.2.1, pp. 15 through 17 (June 2017, amended March 2020).

Strength	Qualities of Identity Evidence

Strong	• The issuing source of the evidence confirmed the claimed identity through written procedures designed to enable it to form a reasonable belief that it knows the real-life identity of the person. Such procedures are subject to recurring oversight by regulatory or publicly accountable institutions. For example, the Customer Identification Program guidelines established in response to the *USA PATRIOT Act of 2001* or the Red Flags Rule, under section 114 of the *Fair and Accurate Credit Transaction Act of 2003*.
	• The issuing process for the evidence ensured it was delivered into the possession of the individual to whom it relates.
	• The issued evidence contains at least one reference number that uniquely identifies the person to whom it relates.
	• The full name on the issued evidence must be the name by which the person was officially known at the time of issuance. Not permitted are pseudonyms, aliases, an initial for surname, or initials for all given names.
	• The:
	  ○ Issued evidence contains a photograph or biometric template (of any modality) of the person to whom it relates, OR
	  ○ Customer proves possession of an Authenticator Assurance Level 2 authenticator, or equivalent, bound to an Identity Assurance Level 2 identity, at a minimum.
	• Where the issued evidence includes digital information, that information is protected using approved cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the claimed issuing source to be confirmed.
	• Where the issued evidence contains physical security features, it requires proprietary knowledge and proprietary technologies to be able to reproduce it.
	• The evidence is unexpired.

Strength	Qualities of Identity Evidence
Superior	• The issuing source of the evidence confirmed the claimed identity by following written procedures designed to enable it to have high confidence the source knows the individual's real-life identity. Such procedures are subject to recurring oversight by regulatory or publicly accountable institutions. • The issuing source visually identified the customer and performed further checks to confirm that person's existence. • The issuing process for the evidence ensured it was delivered into the possession of the person to whom it relates. • The evidence contains at least one reference number that uniquely identifies the person to whom it relates. • The full name on the evidence must be the name the person was officially known by at the time of issuance. Not permitted are pseudonyms, aliases, an initial for surname, or initials for all given names. • The evidence contains a photograph of the person to whom it relates. • The evidence contains a biometric template (of any modality) of the person to whom it relates. • The evidence includes digital information, the information is protected using approved cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the issuing source to be confirmed. • The evidence includes physical security features that require proprietary knowledge and proprietary technologies to be able to reproduce it. • The evidence is unexpired.

Appendix F– AGENCY COMMENTS

SOCIAL SECURITY

MEMORANDUM

Date: September 21, 2023 Refer To: TQA-1

To: Gail S. Ennis
Inspector General

From: Scott Frey
Chief of Staff

Subject: Office of the Inspector General Summary Draft Report, "Digital Identity in *my* Social Security" (142307) — INFORMATION

Thank you for the opportunity to review the draft report. We agree with the recommendations.

Please let me know if I can be of further assistance. You may direct staff inquiries to Trae Sommer at (410) 965-9102.

Mission: The Social Security Office of the Inspector General (OIG) serves the public through independent oversight of SSA's programs and operations.

Report: Social Security-related scams and Social Security fraud, waste, abuse, and mismanagement, at oig.ssa.gov/report.

Connect: OIG.SSA.GOV

Visit our website to read about our audits, investigations, fraud alerts, news releases, whistleblower protection information, and more.

Follow us on social media via these external links:

Twitter: @TheSSAOIG

Facebook: OIGSSA

YouTube: TheSSAOIG

Subscribe to email updates on our website.