OFFICE OF
THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

THE SOCIAL SECURITY ADMINISTRATION'S eAUTHENTICATION PROCESS

October 2011 A-14-11-11115

AUDIT REPORT

Mission

By conducting independent and objective audits, evaluations and investigations, we inspire public confidence in the integrity and security of SSA’s programs and operations and protect them against fraud, waste and abuse. We provide timely, useful and reliable information and advice to Administration officials, Congress and the public.

Authority

The Inspector General Act created independent audit and investigative units, called the Office of Inspector General (OIG). The mission of the OIG, as spelled out in the Act, is to:

- **Conduct and supervise independent and objective audits and investigations relating to agency programs and operations.**
- **Promote economy, effectiveness, and efficiency within the agency.**
- **Prevent and detect fraud, waste, and abuse in agency programs and operations.**
- **Review and make recommendations regarding existing and proposed legislation and regulations relating to agency programs and operations.**
- **Keep the agency head and the Congress fully and currently informed of problems in agency programs and operations.**

To ensure objectivity, the IG Act empowers the IG with:

- **Independence to determine what reviews to perform.**
- **Access to all information necessary for the reviews.**
- **Authority to publish findings and recommendations based on the reviews.**

Vision

We strive for continual improvement in SSA’s programs, operations and management by proactively seeking new ways to prevent and deter fraud, waste and abuse. We commit to integrity and excellence by supporting an environment that provides a valuable public service while encouraging employee development and retention and fostering diversity and innovation.

SOCIAL SECURITY

MEMORANDUM

Date: October 14, 2011 Refer To:

To: The Commissioner

From: Inspector General

Subject: The Social Security Administration's eAuthentication Process (A-14-11-11115)

OBJECTIVE

Our objective was to determine whether the Social Security Administration's (SSA) current and proposed electronic authentication (eAuthentication) process[1] creates a strong, secure authentication protocol that meets Federal guidelines and standards. For this review, we focused on citizen-to-government Internet applications.[2],[3]

BACKGROUND

SSA is expanding its Internet services to guide the public toward performing more business electronically. Some Internet applications involve the exchange of personally identifiable information (PII)[4] between SSA and the public. According to SSA's Intranet site, these services are more useful and attractive but carry a greater risk of inappropriate disclosure.

[1] eAuthentication is the process of establishing confidence in user identities electronically presented to an information system.

[2] The Agency defines a citizen-to-government Internet application as an application that transacts business between a human and a machine rather than from one machine to another machine.

[3] The Office of Management and Budget (OMB) uses the phrase "user-to-agency" for "citizen-to-government" information system applications. OMB, M-04-04, *E-Authentication Guidance for Federal Agencies,* Attachment A, Section 2.3, Step 4 (December 16, 2003).

[4] OMB defines the term PII as ". . . any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information that is linked or linkable to an individual." OMB, M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, page 1, footnote 1 (July 12, 2006).

The Agency's Internet site supports several types of online Web services: government-to-government, business-to-government, and citizen-to-government applications. We determined that SSA had 22 citizen-to-government Internet applications in place at the time of our review (see Appendix B).

In December 2003, OMB issued guidance to ensure the protection of security and privacy for online Government services.[5] The guidance requires that agencies review new and existing electronic transactions to ensure the eAuthentication processes implemented provided the appropriate level of assurance.[6] Further, the guidance established and described four levels of identity authentication assurance for electronic Government transactions.[7]

- Level 1: Little or no confidence in the asserted identity's validity.
- Level 2: Some confidence in the asserted identity's validity.
- Level 3: High confidence in the asserted identity's validity.
- Level 4: Very high confidence in the asserted identity's validity.

The Agency determined it had 1 Level 1, 14 Level 2, and 3 Level 3 citizen-to-government Internet applications.[8] SSA did not have a Level 4 citizen-to-government Internet application.

Authentication is not required for Level 1 Internet applications. We determined that SSA has implemented a process that was consistent with Federal guidelines and standards for Level 2 authentication. The Agency stated that it did not have an authentication protocol for Level 3 applications, but planned to implement a protocol that will be compliant. According to OMB guidance,[9] to determine the appropriate assurance levels, agencies must use the following steps.

[5] OMB, M-04-04, supra.

[6] OMB, M-04-04, supra, Attachment A at § 1.1.

[7] OMB, M-04-04, supra, Attachment A at § 2.1.

[8] During the fieldwork phase of our review, we were not provided documentation for four citizen-to-government Internet applications. They were *the Medicare Replacement Card, Replacement 1099, Public Fraud Reporting Form,* and *Child Disability Report*. After the issuance of the discussion draft report, an authentication risk assessment (ARA) for the *Public Fraud Reporting Form* application was completed and SSA found the authentication level for this application is Level 1. An ARA is an SSA-defined term that is synonymous with the OMB term for 'risk assessment.' In addition, the *Social Security Statement Internet* application was removed from the production environment in March 2011 and authentication reassessments were completed for the *Internet Change of Address and Internet Direct Deposit* citizen-to-government applications. Both applications are now OMB Level 2 applications.

[9] OMB, M-04-04, supra, Attachment A at § 2.3.

1. **Conduct** a risk assessment of the e-government system.
2. **Map**[10] identified risks to the required assurance level.
3. **Select** technology based on the National Institute of Standards and Technology (NIST) eAuthentication technical guidance.[11]
4. **Validate** that the implemented system achieved the required assurance level after release to production.
5. **Periodically** reassess the information system to determine technology refresh requirements.

To accomplish our objectives, we limited our work to interviewing SSA employees in the Office of Open Government (OOG); reviewing applicable Federal laws and regulations; and examining ARAs and Privacy Impact Assessments. Our review was limited to evaluating the process SSA had in place to implement authentication protocols for online citizen-to-government Internet applications. We did not test the Agency's access controls for citizen-to-government applications. We will test application controls in future audits. Therefore, we do not comment on the security of these Internet applications. See Appendix C for additional information regarding our background, scope, and methodology.

RESULTS OF REVIEW

SSA had taken steps to implement an eAuthentication process that included key elements needed to create a strong, secure authentication protocol for Level 2 citizen-to-government Internet applications. For example, SSA had adopted an acceptable methodology to conduct ARAs and implemented a process that validates the identity of OMB Level 2 Internet application users.[12] The Agency was developing an authentication protocol for future Level 3 citizen-to-government Internet applications that will meet Federal guidelines and standards. However, we identified areas that needed improvement in the Agency's eAuthentication process to ensure compliance with Federal guidelines and standards.

- Four citizen-to-government Internet applications did not have documentation reflecting that ARAs were conducted as required.[13]

[10] Mapping is the process of matching potential impact outcomes to appropriate assurance levels.

[11] The selection of technology referred to in OMB M-04-04, Section 2.3, step 3 will be based on NIST eAuthentication guidance found in Special Publication (SP) 800-63, Version 1.0.2, *Electronic Authentication Guideline*, Chapters 5 and 8 (April, 2006). An amendment to this guidance is currently in Draft. See NIST SP 800-63-1, *Electronic Authentication Guideline* (December 8, 2008).

[12] OMB, M-04-04, § 2.3 and NIST SP 800-63, Version 1.0.2. See Footnote 11.

[13] OMB, M-04-04, supra, Attachment A at § 2.3.

- Four citizen-to-government Internet applications did not have sufficient documentation showing that risks were mapped to applicable assurance levels as required.[14]
- SSA did not have a NIST-compliant methodology that can provide Level 3 assurance for citizen-to-government Internet applications as required.[15]
- SSA did not have a process to validate and document that citizen-to-government Internet applications achieved their required assurance level after release to production as required.[16]
- SSA did not periodically reassess the information system for 11 citizen-to-government Internet applications to ensure that identity authentication requirements continue to be valid in light of technology changes or changes in Agency business processes as required.[17]

Four Citizen-To-Government Internet Applications Did Not Have Documentation Reflecting That Authentication Risk Assessments Were Conducted as Required

We were unable to determine whether an ARA was completed for 4[18] of SSA's 22 citizen-to-government Internet applications. We reviewed 12 ARAs[19] that addressed 18 of the 22 applications. We requested documentation for the four remaining applications, but no documentation was available. OOG staff commented that before January 2009, there was no standard process in place for conducting an ARA, and some projects went through the systems development lifecycle without an ARA.

OMB requires that agencies conduct a risk assessment of e-government systems to ensure authentication processes provide the appropriate level of assurance.[20] We found no documentation existed that verified an ARA was completed for four SSA

[14] Id.

[15] Id. NIST e-authentication guidance is found in Special Publication (SP) 800-63, Version 1.0.2, *Electronic Authentication Guideline*, Chapter 8, section 8.2.3 (April 2006). An amendment to this guidance is in Draft. See NIST SP 800-63-1, *Electronic Authentication Guideline* (December 8, 2008).

[16] See OMB, M-04-04, supra, Attachment A at § 2.3.

[17] Id.

[18] During the fieldwork phase of our review, an ARA could not be located for four applications. They were the *Medicare Replacement Card*, *Replacement 1099*, *Public Fraud Reporting Form*, and *Child Disability Report*. After the issuance of the discussion draft report, an ARA for the *Public Fraud Reporting Form* application was completed and SSA found the authentication level for this application is Level 1.

[19] Some ARAs addressed more than a single citizen-to-government Internet application. For example, the *Internet Social Security Benefit Application* ARA addressed the *Retirement*, *Spouse*, *Disability*, and the *Medicare-Only* applications.

[20] OMB, M-04-04, supra Attachment A, at § 2.3.

citizen-to-government Internet applications. Therefore, SSA was not compliant with Federal requirements[21] for these four Internet applications. Moreover, there was no assurance that SSA implemented appropriate security measures for user identity authentication for these four Internet applications. Consequently, these four applications may not have the appropriate authentication. We recommend SSA perform risk assessments and retain documentation that demonstrates required ARAs were conducted for these four citizen-to-government Internet applications.

Four Citizen-to-Government Internet Applications Did Not Have Sufficient Documentation Showing That Risks Were Mapped to Applicable Assurance Levels as Required

According to OMB, as part of the ARA process, agencies are required to 'map' identified risks to their appropriate assurance level.[22] This process involves summarizing the risks inherent in the transaction process assessed in terms of potential harm and/or impact and likelihood of occurrence. Agencies link the assessment outcomes to the appropriate assurance levels. Quantified results are mapped in terms of their impact as, not applicable, low, moderate, or high. This step determines the appropriate assurance level for the application or transaction. The assurance level assigned determines the security protocol needed to authenticate users to the application.

During our review of SSA's 12 ARAs, we found the documentation insufficient to support that risks were mapped to the appropriate assurance levels for 4[23] citizen-to-government Internet applications. As a result, we concluded the Agency's process was not fully compliant with Federal requirements[24] for these four citizen-to-government applications. OOG staff commented that before January 2009, mapping was conducted but was not consistently documented as part of the ARA process for these four citizen-to-government Internet applications. Consequently, there was no assurance that these four citizen-to-government Internet applications have appropriate authentication protocol in place for users. Lack of an appropriate authentication protocol could result in unauthorized use and possible release of information to the wrong individual. We recommend SSA map identified risks to applicable assurance levels for these four citizen-to-government Internet applications and retain documentation that demonstrates mapping was completed.

[21] Id.

[22] OMB, M-04-04, supra, Attachment A at § 2.3.

[23] The four applications are the applications for which ARAs could not be located.

[24] Id. OMB, M-04-04, supra, Attachment A at § 2.3.

SSA Did Not Have a NIST-Compliant Authentication Protocol for Level 3 Citizen-to-Government Internet Applications

During our review, we identified three SSA citizen-to-government Internet applications[25] that were assigned a Level 3 assurance rating. We determined that SSA did not have a NIST-compliant authentication protocol for these Level 3 citizen-to-government Internet applications. OMB requires that agencies select and implement technology solutions to determine an individual's identity based on NIST eAuthentication technical guidance.[26] After an application's assurance level has been determined, agencies should use NIST eAuthentication guidance to identify and implement the appropriate technical solution needed for user remote authentication.[27] An OMB risk assurance Level 3 rating requires the implementation of a multi-factor remote network authentication protocol.[28] At this level, procedures to determine an individual's identity require verification of identifying materials and information[29] as well as the user's possession of a key or a one-time password.[30]

In anticipation of future Level 3 citizen-to-government Internet applications, the Agency is seeking a compliant solution.[31] The original release date for SSA's new eAuthentication (eA) system was June 2011. The Agency anticipates releasing the eA system in calendar year 2012. Therefore, we recommend SSA reassess the three Level 3 applications and select an authentication technology based on the NIST

[25] The three SSA citizen-to-government Internet applications assigned a Level 3 assurance rating are the *Social Security Statement*, *Change of Address* (password), and *Direct Deposit* applications. After our fieldwork ended, the Agency removed the *Social Security Statement* Internet application from the production environment in March 2011 and authentication reassessments were completed for the *Internet Change of Address* and *Internet Direct Deposit* citizen-to-government applications. Both reassessed applications are now Level 2 applications.

[26] NIST, SP 800-63, Version 1.0.2, supra, Chapter 8, Section 8.2. The amended NIST guidance is in Draft. NIST SP 800-63-1, *Electronic Authentication Guideline* (December 8, 2008). Also see OMB, M-04-04, supra, Attachment A at § 2.3, Step 3.

[27] OMB, M-04-04, supra, Attachment A at § 2.3, Step 3.

[28] NIST, SP 800-63, Version 1.0.2, supra, Chapter 6, section 6.2. The amended NIST guidance is in Draft. NIST SP 800-63-1, *Electronic Authentication Guideline* (December 8, 2008).

[29] Id. According to NIST, SP 800-63, Version 1.0.2, Chapter 5, section 5.2, identifying materials and information include something you have and something you know that only you possess. For example, the pin and password assigned to a user during the registration process. This is a single-factor remote authentication protocol. When you add the requirement of the user having to provide a key or one-time password, you add an additional authentication level, which then becomes a multi-factor level protocol.

[30] NIST, SP 800-63, Version 1.0.2, supra, Chapter 6, section 6.2.

The amended NIST guidance is currently in Draft. See NIST SP 800-63-1, *Electronic Authentication Guideline* (December 8, 2008).

[31] According to OOG personnel, the eA system will meet the multi-factor remote network authentication requirement for OMB Level 2 and 3 applications.

eAuthentication technical guidance. Further, we recommend SSA continue to develop and implement the eA system or an appropriate authentication protocol to help secure the Agency's future Level 3 citizen-to-government Internet applications.

SSA Did Not Have a Process to Validate and Document Citizen-to-Government Internet Applications Achieved Their Required Assurance Level After Release to Production

We determined that none of the 22 citizen-to-government Internet applications were validated as required by Federal guidelines. According to OMB, subsequent to implementation, agencies are required to validate that the information system has operationally achieved the required assurance level.[32] Because some implementations create or compound particular risks, agencies should conduct a final, post-implementation validation to confirm the system achieved the required assurance level for the citizen-to-government process.[33] OOG personnel stated there was no formal process in place to address this requirement. OOG personnel also commented that it evaluates the online applications and provides feedback on evaluation plans that business sponsors create and maintain. In addition, OOG personnel stated that they monitor application activity for 30 to 60 days after release to production, to ensure the application is functioning as intended. However, OOG management stated that because of a lack of resources, stand-alone documentation to support this activity was not available.

Although SSA monitors an application after implementation, the Agency cannot guarantee that appropriate security measures were implemented to adequately protect sensitive electronic transaction data from possible inappropriate disclosure. We recommend SSA establish a process that validates and documents that all implemented citizen-to-government Internet applications have operationally achieved their required assurance level after release to production.

[32] OMB M-04-04, supra, Attachment A, at § 2.3, Step 4.

[33] Id.

SSA Did Not Periodically Reassess the Information System for 11 Citizen-to-Government Internet Applications to Ensure that Identity Authentication Requirements Continue to be Valid in Light of Technology Changes or Changes in Agency Business Processes

We determined that SSA did not conduct required periodic reassessments for 11[34] of 22 citizen-to-government Internet applications. According to OMB, agencies must periodically reassess information systems to ensure identity authentication requirements continue to be valid due to changes in technology and agency business processes.[35] [36] OOG staff commented that it performs reassessments when there is a change in the Internet business process, but there has not been enough staff to conduct periodic assessments as part of cyclical reviews. Since the Agency did not reassess its citizen-to-government Internet applications consistently and timely, SSA may not have updated security measures to address unknown security vulnerabilities. We recommend SSA conduct required periodic reassessments, when applicable, for citizen-to-government Internet applications to ensure identity authentication requirements continue to be valid due to changes in technology or Agency business processes.

CONCLUSION AND RECOMMENDATIONS

SSA took steps to implement an eAuthentication process that included key elements needed to create a strong, secure authentication protocol for Level 2 citizen-to-government Internet applications. The Agency is developing an authentication protocol for future Level 3 citizen-to-government Internet applications to meet Federal guidelines and standards. While certain aspects of SSA's eAuthentication process are generally consistent with Federal guidelines, some areas require improvement. Therefore, we recommend that SSA:

1. Perform risk assessments and retain documentation that demonstrates the completion of required ARAs for the four citizen-to-government Internet applications identified in this report.

[34] The 11 citizen-to-government applications for which required periodic reassessments were not conducted are the *Social Security Statement*, *Retirement Estimator*, *Retirement Application*, *Spouse Application*, *Disability Application, Medicare-Only Application, Appeal Disability Report-3441, Change of Address (PIN and Password), Change of Address (Knowledge Based Authentication), Direct Deposit (PIN and Password),* and *Application Status* applications. After the completion of the fieldwork phase of our review, the Agency removed the *Social Security Statement* Internet application from the production environment in March 2011 and authentication reassessments were completed for the *Internet Change of Address* and Internet *Direct Deposit* citizen-to-government applications.

[35] OMB, M-04-04, supra, Attachment A at § 2.3, Step 5.

[36] Id. Technology changes can occur because of new products and innovations. Business processes can change because of new or obsolete functionality. Changes can also occur within processes or the processing environment that can have an impact on an application.

2. Map identified risks to applicable assurance levels for the four citizen-to-government Internet applications identified in this report, and retain documentation that demonstrates mapping was completed.

3. Reassess the three Level 3 applications identified in this review, and select an authentication technology based on the NIST eAuthentication technical guidance.

4. Continue to develop and implement the eA system or an appropriate authentication protocol to help secure the Agency's future Level 3 citizen-to-government Internet applications.

5. Establish a process that validates and documents that all implemented citizen-to-government Internet applications have operationally achieved their required assurance level after release to production.

6. Conduct required periodic reassessments, when applicable, for citizen-to-government Internet applications to ensure identity authentication requirements continue to be valid in light of changes in technology or Agency business processes.

AGENCY COMMENTS

SSA agreed with our recommendations. See Appendix D for the Agency's comments.

Patrick P. O'Carroll, Jr.

Appendices

Appendix A

Acronyms

ARA	Authentication Risk Assessment
AW	Authentication Workgroup
eA	Electronic Authentication System
eAuthentication	Electronic Authentication
KBA	Knowledge Based Authentication
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OOG	Office of Open Government
PII	Personally Identifiable Information
SP	Special Publication
SSA	Social Security Administration

Appendix B

Social Security Administration Citizen-to-Government Internet Applications

Application	Last Date Assessed	Office of Management and Budget Authentication Level
Social Security Statement	02/11/2005	Level 3[1]
Spanish Retirement Estimator	New Application	Level 2
Retirement Estimator	10/13/2005	Level 2
Retirement Application	01/16/2008	Level 2
Spouse Application	01/16/2008	Level 2
Disability Application	01/16/2008	Level 2
Medicare-only Application	01/16/2008	Level 2
Revised Adult Disability Report–i3368	06/02/2009	Level 2
Child Disability Report-3820		
Appeal Disability Report-3441	03/06/2007	Level 2
Proof of Income Letter	06/01/2010	Level 2
Check Your Benefits	07/02/2009	Level 2
Change of Address (PIN and Password)	06/09/2011	Level 2
Change of Address (Knowledge Based Authentication)	02/13/2005	Level 2
Direct Deposit (PIN and Password)	06/10/2011	Level 2
Medicare Replacement Card		
i1020 (Applicant and 3rd Party)	03/23/2011	Level 2
Replacement 1099		
Application Status	01/10/2007	Level 2
Special Notice Option	11/10/2009	Level 2
iAppointment	06/04/2010	Level 1
Public Fraud Reporting Form	06/15/2011	Level 1

[1] After our fieldwork ended, SSA removed the *Social Security Statement* Internet application from the production environment in March 2011 and completed authentication risk reassessments for the *Internet Change of Address* and *Internet Direct Deposit* citizen-to-government applications. Both reassessed applications are now Level 2 applications. Furthermore, an ARA for the *Public Fraud Reporting Form* application was completed and SSA found the authentication level for this application is Level 1.

Background, Scope, and Methodology

Background

In May 2008, the Office of Notice Improvement and Authentication and the Authentication Workgroup initiated a detailed review of the Authentication Risk Assessment (ARA) process. Based on this review, the ARA process was changed. For example, in July 2008, as part of the ARA process, the Office of Notice Improvement and Authentication began using the Electronic Risk Assessment tool that was created by the General Services Administration and Carnegie Mellon's Software Engineering Institute.

Before July 2008 -- ARA Process

- A group of key stakeholders met to review the proposed business processes.
- A qualitative approach to assess risk was used.
- Each stakeholder assessed risk differently based on varying interpretations of the Office of Management and Budget Memorandum M-04-04 guidelines. The risk assessment relied on a panel of stakeholders reaching a consensus on the impact categories, but the panel often disagreed and could not reach consensus. In these cases, the component with the highest assessment determined the overall assurance level.

After July 2008 -- ARA Process

- Risk assessments are conducted using the Electronic Risk Assessment tool.
- The Authentication Workgroup, in conjunction with the business sponsor, conducts the ARA.
- A quantitative approach versus a qualitative approach is used to assess risk.
- The definitions of "Low," "Moderate," and "High" impact were included to better align with the Social Security Administration's (SSA) business processes.
- Examples of each risk category were included to provide context for voters.
- Voting results are averaged so that each stakeholder's vote is counted and each stakeholder has equal input into the outcome of the assessment.

Scope and Methodology

To accomplish our objectives, we

- reviewed applicable Federal laws and regulations and applicable SSA policies and procedures;
- interviewed Agency staff from the Office of Open Government;
- examined Privacy Impact Assessments;[1] and
- examined ARAs conducted by the Office of Open Government.

We did not perform penetration testing of the Agency's citizen-to-government applications; therefore, we do not comment on the security of these Websites.

We performed our audit at SSA Headquarters from October 2010 to March 2011. We conducted this review in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the review to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our review objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our review objectives.

[1] A Privacy Impact Assessment (PIA) is an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic system, and (iii) to examine and evaluate protections and alternate processes for handling information to mitigate potential privacy risks. The Office of Management and Budget, M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, Attachment A, Section II.A.f, September 26, 2003.

Appendix D

Agency Comments

SOCIAL SECURITY

MEMORANDUM

Date: August 25, 2011 Refer To: S1J-3

To: Patrick P. O'Carroll, Jr.
Inspector General

From: Dean S. Landis /s/
Deputy Chief of Staff

Subject: Office of the Inspector General Draft Report, "The Social Security Administration's eAuthentication Process" (A-14-11-11115)--INFORMATION

Thank you for the opportunity to review the draft report. Please see our attached comments.

Please let me know if we can be of further assistance. You may direct staff inquiries to Frances Cord at (410) 966-5787.

Attachment

COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL (OIG) DRAFT REPORT, "THE SOCIAL SECURITY ADMINISTRATION'S eAUTHENTICATION PROCESS" (A-14-11-11115)

GENERAL COMMENT

We have greatly improved our Authentication Risk Assessment (ARA) process in recent years. We use the Electronic Risk and Requirements Assessment (e-RA) tool, which is compliant with Office of Management and Budget guidelines, to identify the risks associated with insufficient authentication of users and to formally guide us through the assessment process. We also assess the worst-case scenario and the likelihood that a scenario would happen. Finally, we initiated a dedicated eAuthentication workgroup to provide an overlying governance structure for the ARA process.

RESPONSE TO RECOMMENDATIONS

Recommendation 1

Perform risk assessments and retain documentation that demonstrates the completion of required ARAs for the four citizen-to-government Internet applications identified in this report.

Response

We agree that there are three applications in need of risk assessments. We are planning to conduct the required ARAs for Medicare Replacement Card, Replacement 1099, and Child Disability Report. After conducting the ARA on the OIG Public Fraud Reporting Form application, we determined it does not require authentication because there is no applicable level of risk. We provided documentation to OIG supporting this determination on July 13, 2011.

Recommendation 2

Map identified risks to applicable assurance levels for the four citizen-to-government Internet applications identified in this report, and retain documentation that demonstrates mapping was completed.

Response

We agree. We will continue our practice of mapping an application as part of our assessment. When we conduct the ARA for Medicare Replacement Card, Replacement 1099, and Child Disability Report, we will map the identified risks as part of the process.

Recommendation 3

Reassess the three Level 3 applications identified in this review, and select an authentication technology based on the National Institute of Standards and Technology (NIST) eAuthentication technical guidance.

Response

We agree. Using the e-RA tool, we completed our reassessment of the Change of Address and Direct Deposit applications and determined they are at a Level 2. The third application, Social Security Statement, is no longer in production. The business process for the upcoming Online Statement application is complete, and we determined the application is at a Level 2. We properly documented the authentication assessment for all three applications.

We consider this recommendation closed for tracking purposes.

Recommendation 4

Continue to develop and implement the Citizen Authentication Initiative or an appropriate authentication protocol to help secure the Agency's future Level 3 citizen-to-government Internet applications.

Response

We agree. Currently, we do not have any Level 3 citizen-to-government applications. We continue to work on this initiative and anticipate providing the appropriate Level 3 technology as an option for users who want extra security to be available in the future.

Recommendation 5

Establish a process that validates and documents that all implemented citizen-to-government Internet applications have operationally achieved their required assurance level after release to production.

Response

We agree. We are developing a new authentication system that will provide support to access eServices applications at a Level 2 or Level 3, which are consistent with the requirements of NIST 800-63. In addition, we will monitor the integrity of the new credentials to validate and document the required assurance levels.

Recommendation 6

Conduct required periodic reassessments, when applicable, for citizen-to-government Internet applications to ensure identity authentication requirements continue to be valid in light of changes in technology or agency business processes.

Response

We agree. We conduct ARA reassessments when we become aware of changes in the business process of an Internet application. In addition, we created a maintenance chart to perform periodic reassessments as we move applications to our new electronic Authentication (eA) system.

Appendix E

OIG Contacts and Staff Acknowledgments

OIG Contacts

Brian Karpe, Director, Information Technology Audit Division

Mary Ellen Moyer, Audit Manager

Acknowledgments

In addition to those named above:

Harold Hunter, Auditor in Charge

For additional copies of this report, please visit our Website http://oig.ssa.gov/ at or contact the Office of the Inspector General's Public Affairs Staff Assistant at (410) 965-4518. Refer to Common Identification Number A-14-11-11115.

DISTRIBUTION SCHEDULE

Commissioner of Social Security

Chairman and Ranking Member, Committee on Ways and Means

Chief of Staff, Committee on Ways and Means

Chairman and Ranking Minority Member, Subcommittee on Social Security

Majority and Minority Staff Director, Subcommittee on Social Security

Chairman and Ranking Minority Member, Committee on the Budget, House of Representatives

Chairman and Ranking Minority Member, Committee on Oversight and Government Reform

Chairman and Ranking Minority Member, Committee on Appropriations, House of Representatives

Chairman and Ranking Minority, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations,
House of Representatives

Chairman and Ranking Minority Member, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Committee on Finance

Chairman and Ranking Minority Member, Subcommittee on Social Security Pensions and Family Policy

Chairman and Ranking Minority Member, Senate Special Committee on Aging

Social Security Advisory Board

Overview of the Office of the Inspector General

The Office of the Inspector General (OIG) is comprised of an Office of Audit (OA), Office of Investigations (OI), Office of the Counsel to the Inspector General (OCIG), Office of External Relations (OER), and Office of Technology and Resource Management (OTRM). To ensure compliance with policies and procedures, internal controls, and professional standards, the OIG also has a comprehensive Professional Responsibility and Quality Assurance program.

Office of Audit

OA conducts financial and performance audits of the Social Security Administration's (SSA) programs and operations and makes recommendations to ensure program objectives are achieved effectively and efficiently. Financial audits assess whether SSA's financial statements fairly present SSA's financial position, results of operations, and cash flow. Performance audits review the economy, efficiency, and effectiveness of SSA's programs and operations. OA also conducts short-term management reviews and program evaluations on issues of concern to SSA, Congress, and the general public.

Office of Investigations

OI conducts investigations related to fraud, waste, abuse, and mismanagement in SSA programs and operations. This includes wrongdoing by applicants, beneficiaries, contractors, third parties, or SSA employees performing their official duties. This office serves as liaison to the Department of Justice on all matters relating to the investigation of SSA programs and personnel. OI also conducts joint investigations with other Federal, State, and local law enforcement agencies.

Office of the Counsel to the Inspector General

OCIG provides independent legal advice and counsel to the IG on various matters, including statutes, regulations, legislation, and policy directives. OCIG also advises the IG on investigative procedures and techniques, as well as on legal implications and conclusions to be drawn from audit and investigative material. Also, OCIG administers the Civil Monetary Penalty program.

Office of External Relations

OER manages OIG's external and public affairs programs, and serves as the principal advisor on news releases and in providing information to the various news reporting services. OER develops OIG's media and public information policies, directs OIG's external and public affairs programs, and serves as the primary contact for those seeking information about OIG. OER prepares OIG publications, speeches, and presentations to internal and external organizations, and responds to Congressional correspondence.

Office of Technology and Resource Management

OTRM supports OIG by providing information management and systems security. OTRM also coordinates OIG's budget, procurement, telecommunications, facilities, and human resources. In addition, OTRM is the focal point for OIG's strategic planning function, and the development and monitoring of performance measures. In addition, OTRM receives and assigns for action allegations of criminal and administrative violations of Social Security laws, identifies fugitives receiving benefit payments from SSA, and provides technological assistance to investigations.