While Progress Is Being Made on Digital Identity Requirements, Completion Dates to Achieve Compliance With Identity Proofing Standards Have Not Been Established

March 23, 2020

Reference Number: 2020-20-012

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Redaction Legend:
2 = Law Enforcement Techniques/Procedures and Guidelines for Law Enforcement Investigations or Prosecutions

Phone Number / 202-622-6500
E-mail Address / TIGTACommunications@tigta.treas.gov
Website / http://www.treasury.gov/tigta

To report fraud, waste, or abuse, call our toll-free hotline at:

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

Treasury Inspector General for Tax Administration
P.O. Box 589
Ben Franklin Station
Washington, D.C. 20044-0589

Information you provide is confidential and you may remain anonymous.

WHILE PROGRESS IS BEING MADE ON DIGITAL IDENTITY REQUIREMENTS, COMPLETION DATES TO ACHIEVE COMPLIANCE WITH IDENTITY PROOFING STANDARDS HAVE NOT BEEN ESTABLISHED

Highlights

Final Report issued on March 23, 2020

Highlights of Reference Number: 2020-20-012 to the Commissioner of Internal Revenue.

IMPACT ON TAXPAYERS

Advances in technology have provided the IRS an opportunity to be more responsive to the taxpayer's need for its services. However, a new set of challenges has emerged because information about individuals has become more widely available through social media and breaches of Personally Identifiable Information. As a result, the IRS needs to work toward improving its public-facing applications to ensure that taxpayers who want access to IRS online services have verified their identities and can access IRS resources in a secure manner.

WHY TIGTA DID THE AUDIT

This audit was initiated to evaluate the IRS's identity proofing capabilities for secure electronic authentication to online applications. Identity proofing is ensuring that users who interact with an entity over open networks, *i.e.*, the Internet, are who they claim to be.

WHAT TIGTA FOUND

In June 2017, the National Institute of Standards and Technology issued updated guidance on identity proofing in Special Publication 800-63-3, *Digital Identity Guidelines*.

The IRS is making progress to comply with those guidelines on identity proofing by developing and using a five-step process to determine the required assurance level for each application and by creating a solution to ensure that the applicant is who they claim to be within a stated level of confidence.

However, the IRS may not complete its processes on all applications as scheduled, and it is using compensating controls that include identity proofing and authentication level of assurances based on superseded guidelines for certain applications that require either remote or physical presence for identity proofing. While these compensating controls did not fully meet the requirements, the IRS stated they are the most secure methods to remotely identity proof and authenticate taxpayers until its new digital identity platform is implemented, which is expected to begin being piloted in June 2020.

The IRS has 63 public-facing applications that taxpayers can access from the Internet. As of July 2019, eight (13 percent) of these applications have completed all five steps of the digital identity risk assessment process, while 17 (27 percent) applications have completed four of the steps. The remaining 38 applications are not expected to complete all five steps until January 2020. However, TIGTA is concerned as to whether the IRS can achieve that date given that it took an average of 217 calendar days to complete the eight applications through step five.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Information Officer ensure that the remaining public-facing applications complete all five steps in the digital identity risk assessment process, and that all testing for the digital identity solution is completed and all public-facing applications are migrated to the implemented solution. In addition, the Deputy Commissioner for Operations Support should coordinate with the Department of the Treasury on legislative proposals or policy changes needed to obtain additional assistance from States, Territories, and Federal agencies that issue identifications in identity proofing users.

The IRS agreed with two recommendations and plans to complete the five-step process for the remaining public-facing applications and conduct tests to validate the solution and migrate all applications to the solution as needed. The IRS partially agreed with the third recommendation and will brief the Department of the Treasury on the identity proofing issue.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

March 23, 2020

MEMORANDUM FOR COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – While Progress Is Being Made on Digital Identity Requirements, Completion Dates to Achieve Compliance With Identity Proofing Standards Have Not Been Established (Audit # 201920004)

This report presents the results of our review to evaluate the Internal Revenue Service's (IRS) identity proofing capabilities for secure electronic authentication to online applications. This audit is included in our Fiscal Year 2020 Annual Audit Plan and addresses the major management challenge of Security Over Taxpayer Data and Protection of IRS Resources.

Management's complete response to the draft report is included as Appendix VII.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. If you have any questions, please contact me or Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Abbreviations

CSP	Credential Service Provider
DIRA	Digital Identity Risk Assessment
IAL	Identity Assurance Level
IAM	Identity and Access Management
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
SADI	Secure Access Digital Identity
SOP	Standard Operating Procedures
SP	Special Publications
TIGTA	Treasury Inspector General for Tax Administration

Background

Advances in technology have allowed for more reliable and secure digital interaction capabilities on business transactions, offering the Federal Government an opportunity to be more responsive to the public's need for its services. A new set of challenges has emerged with this opportunity because information about individuals has become more widely available through social media and breaches of Personally Identifiable Information.[1]

In June 2017, the National Institute of Standards and Technology (NIST) issued NIST Special Publication (SP) 800-63-3, *Digital Identity Guidelines*,[2] to cover identity proofing and authentication of users (such as employees, contractors, or private individuals) interacting with Federal Government information technology systems over open networks, such as the Internet. Identity proofing's sole objective is to ensure that the applicant is who they claim to be, to a stated level of confidence. This includes presentation, validation, and verification of the minimum attributes necessary to accomplish identity proofing. Digital identity presents a technical challenge because this process often involves verifying individuals' identities and authenticating individual subjects over an open network to access digital Government services. The processes and technologies to establish and use digital identities offer multiple opportunities for impersonation and other attacks.

NIST SP 800-63-3 is split into a suite of documents that include NIST SP 800-63A, *Digital Identity Guidelines: Enrollment and Identity Proofing*, for the specific purpose of providing requirements for enrollment and identity proofing of applicants who wish to gain access to resources in any instance. This suite as a whole is referred to as "the guidelines" that relying parties, such as the Internal Revenue Service (IRS), are required to use. NIST SP 800-63A guidelines established three identity assurance levels (IAL).

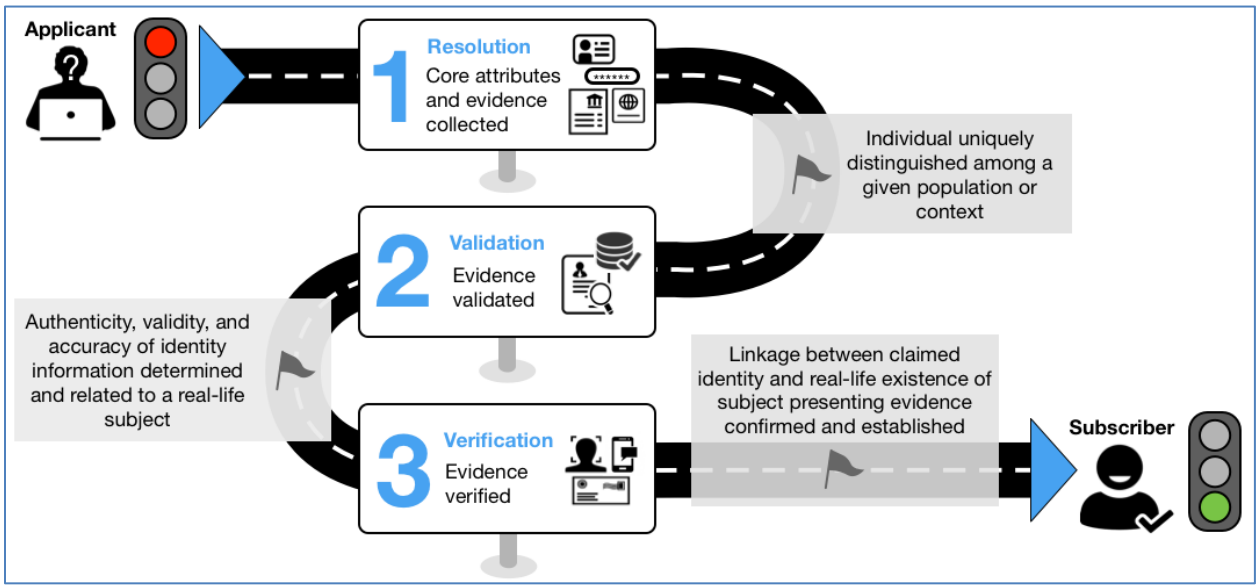
- IAL1 – There is no requirement to link the applicant to a specific real-life identity. Any attributes provided in conjunction with the subject's activities are self-asserted, which are neither validated nor verified.
- IAL2 – Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. IAL2 introduces the need for either remote or physically present identity proofing.

[1] See Appendix VI for a glossary of terms.
[2] These guidelines describe the risk management processes to select appropriate digital identity services and the details to implement identity assurance, authenticator assurance, and federation assurance levels based on risk. They also supersede NIST SP 800-63-2, *Electronic Authentication Guideline* (August 2013).

- IAL3 – Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained credential service provider (CSP) representative.

Figure 1 shows the process flow of an applicant's journey for identity proofing and enrollment.

Figure 1: Process Flow of an Applicant for Identity Proofing



Source: NIST SP 800-63A.

The expected outcome of identity proofing is to:

- Resolve a claimed identity to a single, unique identity within the context of the population of users the CSP serves.
- Validate that all supplied evidence is correct and genuine, *e.g.*, not counterfeit or stolen.
- Validate that the claimed identity exists in the real world.
- Verify that the claimed identity is associated with the real person supplying the identity evidence.

In the September 2018 House Ways and Means Committee, Oversight Subcommittee Hearing on *The Internal Revenue Service's Taxpayer Online Authentication*, Chairman John Lewis stated the purpose of the hearing was to examine how the IRS confirms taxpayers' identities when they use online services. Chairman Lewis further stated that the process was important to reduce identity theft and refund fraud, and he cited that the growing number of security breaches across the public and private sector often makes it difficult for the agency to identify the real taxpayer. In many cases, criminals combine sensitive taxpayer information that they have stolen from several sources. The thieves use this information to access taxpayers' online accounts. The Treasury Inspector General for Tax Administration (TIGTA) Deputy Inspector General for Audit

informed the Committee that we planned to provide continuing audit coverage of the IRS's efforts to protect the confidentiality of taxpayer data. This audit provides the progress the IRS has made on identity proofing for public-facing online applications.

This review was performed at the IRS Information Technology organization's Applications Development, Identity and Access Management (IAM) and the Cybersecurity, Digital Identity Risk Assessment (DIRA) functions in Lanham, Maryland, and the Privacy, Governmental Liaison, and Disclosure office's Identity Assurance function in Atlanta, Georgia. In addition, we obtained information from two vendors asserting an identity proofing solution in McLean, Virginia, and Washington, D.C., during the period February through August 2019. 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

The IRS is making progress to comply with NIST guidelines on identity proofing by developing and using a process to determine the required assurance level for each application and by creating a solution to ensure that the applicant is who they claim to be within a stated level of confidence. The IRS has 63 public-facing applications[3] that will each need an IAL, as the NIST requires, to permit taxpayers or practitioners access to the online services and capabilities it provides.

The Digital Identity Risk Assessment Process Is Generally Compliant With New Requirements for Identity Proofing, but More Work Is Needed to Fully and Timely Meet Current Standards for Remote and Physical Identity Proofing

Based on our review of documents and discussions with Cybersecurity function officials, we found that the Cybersecurity function implemented the DIRA process and developed a draft DIRA Standard Operating Procedures (SOP) document that outlined the purpose, procedures, and output of each activity within the DIRA process. Cybersecurity function personnel used the draft SOP to perform the DIRA process. The process enables a data-driven approach to identity assurance risk determinations and related implementation for IRS public-facing applications. It seeks to:

- Enable a more objective risk assessment with a data-driven outcome.
- Evolve the risk process to facilitate adoption of NIST SP 800-63-3 guidelines and to adapt to the changing threat landscape.
- Implement repeatable and ongoing risk assessments that are efficient and transparent, and provide accountability in securing the digital taxpayer's experience.

The DIRA process includes the following main components:

- **The DIRA Tool** – The DIRA team uses the DIRA tool to collect, correlate, and analyze transaction data to produce data-driven xALs.[4] It includes information about the application, such as 1) its purpose; 2) the names of the stakeholders; 3) the volume of users of the application; 4) a list of Personally Identifiable Information or other

[3] The IRS identified 64 public-facing applications; however, only 63 were scheduled for the DIRA process to date. Hereafter, we will only address the 63 applications.
[4] When described generically or bundled, NIST SP 800-63-3 guidelines refer to the IAL, authenticator assurance level, and federation assurance level as xAL.

personal/demographic information used in the application and whether the applicant self-asserted or the application discloses the information; 5) a list of tax/Internal Revenue Code Section 6103 information used in the application; 6) the Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems*,[5] rating; and 7) questions about the application and its relationship to tax administration.

In addition, the tool assesses the impact of potential harms that could result from an identity proofing error. Those harms are:

- Personal safety – Could physical injury or death occur?
- Harm to agency programs or public interests – Could the IRS's mission-essential functions be adversely affected?
- Financial loss or agency liability – Would the IRS incur a direct financial loss and/or financial liability? Would the taxpayer or other party incur a direct financial loss?
- Civil or criminal violations – Is there a risk that the IRS would be subjected to civil or criminal violations?
- Unauthorized release of sensitive information – Would the release of personal, government, or commercially sensitive information result in a loss of confidentiality?
- Inconvenience, distress, or damage to standing reputation – Is there potential for damage to the IRS's reputation? Is there potential for inconvenience or distress to the taxpayer or another party, *e.g.*, the taxpayer is unable to file his/her taxes and/or collect a refund(s), or a privacy violation that causes emotional distress? Is there potential for damage to the reputation of the taxpayer or another party?

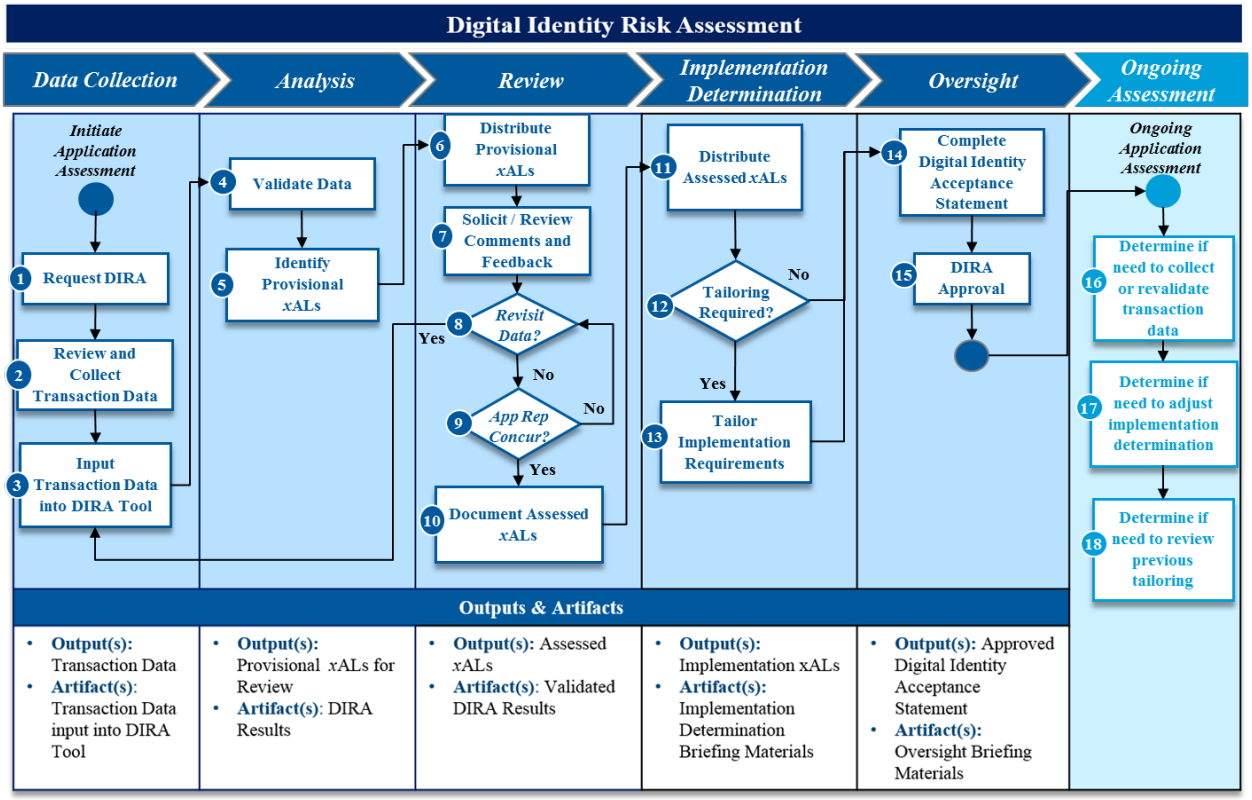
- **DIRA Report** – A compilation of the key identity risk assessment artifacts, which provides a comprehensive record of the DIRA process and includes DIRA results.
- **DIRA Results** – The output of the DIRA tool, which provides the assessed xALs and an overview of the transaction data input.
- **Implementation Determination Briefing Materials** – The context and details identified during the Implementation Determination process, including any required compensating controls. Compensating controls are necessary if a solution is not available to ensure that applicants are who they claim to be.
- **Digital Identity Acceptance Statement** – Per NIST SP 800-63-3, the statement includes the acknowledgment of the assessed xALs, the implementation xALs, and other relevant

[5] U.S. Department of Commerce, Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems* (Feb. 2004).

information. For the IRS, the statement provides a high-level overview of the DIRA process and implementation rationale for the application. The Acceptance Statement receives approval from IRS executives such as the Chief Information Officer, the Chief Privacy Officer, the Small Business/Self-Employed Division and Wage and Investment Division Commissioners, and the application business owner (if other than the two previously named Commissioners).

Figure 2 depicts the DIRA six-step approach.

Figure 2: The DIRA Six-Step Approach



*Source: Cybersecurity DIRA overview dated May 2019. *App Rep – Business Unit Application Representative.*

For the above process, NIST requires 10 elements that are to be strictly followed to conform with its guidelines. We determined that three of the 10 elements did not apply because the IRS is not and does not plan to be a CSP for other Federal agencies.[6] For the remaining seven elements, we

[6] See Appendix V for the DIRA SOP and its compliance with the 10 NIST required elements. However, the IRS considers itself a CSP under the superseded NIST SP 800-63-2 guidelines. As a CSP, the IRS uses the eAuthentication level of assurance 2 and 3 workflow process that involves the Integrated Customer Communications Environment verification, financial verification, and/or telephone verification to issue or register tokens and issue electronic credentials to taxpayers.

confirmed that the IRS included them in the draft DIRA SOP. However, we did identify two requirements in the draft version of the SOP that should be updated prior to it being finalized.

Two requirements within the draft DIRA SOP needed updating

First, we did not identify a requirement for capturing the concurrence of the preoversight and oversight voting decisions. The SOP required the approval of the assessed xAL levels; however, it did not specify that the approval be in writing or documented. The preoversight review team, which consists of the Associate Chief Information Officer, Cybersecurity; the executive from the Identity Assurance function; and an executive from the application business owner, provided their verbal concurrences to the xALs (as documented in meeting minutes). The Oversight Review team had a similar action in its approval of the digital risk assessment statement. However, after our inquiry about the verbal concurrence and at the direction of the Oversight Review team, the DIRA team started using the Microsoft Outlook™ voting button feature to capture each of the preoversight and oversight review team members' concurrences. In addition, reference to the voted concurrence is aligned with each team member's name and title. This process should be included in the DIRA SOP before it is finalized or at the next update.

Second, we had concerns with the vagueness of the "periodic" reassessment as part of the sixth step of the DIRA process that requires an ongoing assessment of the public-facing application. The SOP stated that applications must be reassessed on an ongoing basis to ensure that appropriate xALs are being applied and to validate that the xALs are being consistently implemented. Reassessment will occur on a periodic basis or after event-based triggers, such as a DIRA process change, transaction data change within an application, or risk environment change. The Cybersecurity function had not defined "periodic" because the DIRA process was still being implemented when the procedures were created. Cybersecurity function personnel stated that it did not want to lock in a specific time frame to allow for flexibility as they completed the DIRA process on all the applications.

***Management Action*:** After the completion of our fieldwork, the Director, Security Risk Management, provided the finalized version of the SOP dated August 2019. We reviewed the approved finalized SOP and verified that it included a requirement to capture the concurrences of the preoversight and oversight voting decisions and defined the term "periodic" as an annual reassessment of the public-facing applications for the appropriateness of the xAL designations.

Concerns about compliance with the NIST requirement for remote and physical identity proofing

Our review of the DIRA process also identified concerns about the IRS's ability to comply with the NIST element that requires agencies to demonstrate comparability of any chosen alternative to include compensating controls when the complete set of applicable NIST SP 800-63-3 requirements are not implemented. The IRS's compensating controls include the level of assurance 2 and 3 workflow process for identity proofing and authentication that is based on the superseded NIST SP 800-63-2 guidelines. For the level of assurance 3 workflow process, the

IRS uses four separate steps that collect and confirm distinct sets of information. Users must confirm their identity at each step before the IRS grants access to its online services. This multistep approach provides the IRS with assurance of the taxpayer's identity.

- **********2**********2**********.
- **********2**********2**********.
- **********2**********2**********2**********.
- **********2**********2**********2**********.

**********2**********2**********2**********2**********2**********2**********2**********2**********2**********.

For some context on our concern, much of the information the IRS uses to provide assurance of the taxpayers' identities may have been stolen from the Government and the private sector in the last four calendar years. For example, in Calendar Year 2015, the Office of Personnel Management and its interagency response team concluded that sensitive information, *e.g.*, full name, birth date, home address, and Social Security Number, for approximately 22 million individuals was stolen from its systems. In September 2017, the credit reporting bureau Equifax announced that personal data including individuals' names, Social Security Numbers, birth dates, addresses, and in some cases driver's license numbers had been stolen. A subsequent investigation determined the breach affected approximately 148 million individuals in total.

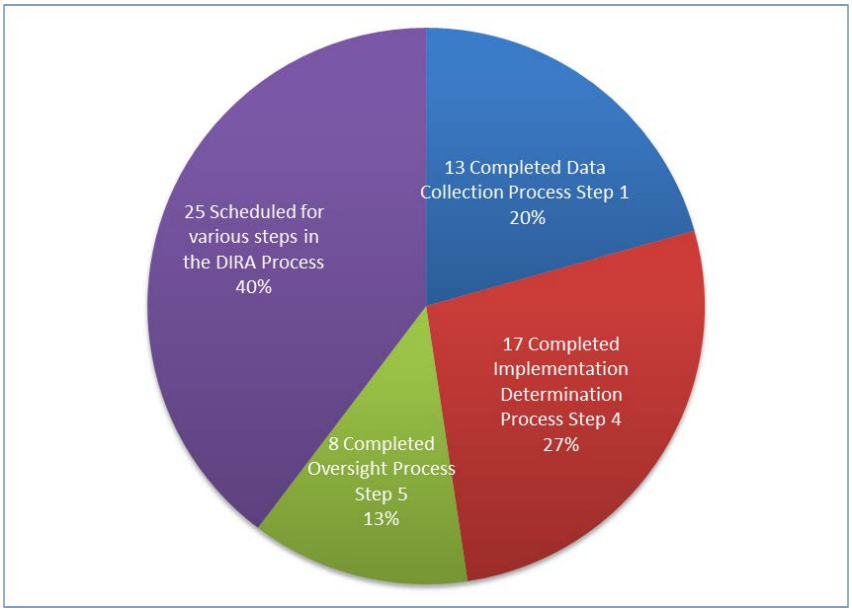
We concluded that neither the level of assurance 2 nor 3 workflow process, which are based on superseded NIST guidelines, are comparable to NIST SP 800-63-3 requirements for the applications designated as IAL2, which introduces the need for either remote or physical presence for identity proofing. The IRS acknowledged that the workflow processes did not fully meet IAL2 standards, but stated they are the most secure methods currently available to remotely identity proof and authenticate taxpayers. The IRS is developing a digital identity solution, which we discuss further in this report; however, the implementation date for the solution to

include all the IRS's public-facing applications is unknown, though the IRS does plan to pilot the solution in June 2020. We are not making any recommendations for the previously mentioned concerns that ultimately affect the security of taxpayer data because we believe the solution for our concerns is intricately involved in the digital identity solution presented later in this report.

Concerns about the timely completion of the DIRA process

The IRS has 63 public-facing applications that taxpayers or practitioners can access from the Internet. Figure 3 shows that, from October 2, 2018, through July 1, 2019, these applications either have been completed or were in varied steps in the DIRA process.

Figure 3: The 63 Public-Facing Applications in Varied Stages of the DIRA Process, as of July 1, 2019



Source: TIGTA analysis of the IRS's 63 public-facing applications.

The Data Collection step of the DIRA process starts by collecting background data and scheduling a meeting with the stakeholders to verify the data. During the Implementation Determination step, stakeholders review briefing materials that include the implementation xALs. The Oversight step features the Chief Information Officer, the Chief Privacy Officer, and the Small Business/Self-Employed Division and the Wage and Investment Division Commissioners' review and approval of the risks that have been identified for each public-facing application and the planned and existing controls to mitigate those risks.

The IRS decided the IAL for the applications that completed steps four and five as either IAL1, which will not require a user to validate or verify his/her identity, or IAL2, which will require a user to complete identity proofing remotely or by being physically present. We attended meetings with the stakeholders and the DIRA team while they were discussing seven of the

25 applications and reviewed the supporting documentation for all 25 applications, such as the initial DIRA reports, that the IRS used to make its decisions. We concur that the designated IALs were appropriate, *i.e.*, six applications at IAL1 and *********2**********.

**********2********** include the Online Accounts application that permits 24 million taxpayers annually to view their balance due amounts, payment histories, and view or obtain transcript-related products; the Get Transcript application, which 16 million taxpayers access annually; and the Identity Protection Personal Identification Number application which 500,000 taxpayers[7] access annually. For the remaining scheduled applications or those that have completed step one, the Cybersecurity function expects them to complete step four by December 2019 and step five by January 2020.

While the IRS is making progress, we are concerned as to whether the IRS can achieve these milestone dates. We analyzed the length of time the IRS took to complete the eight applications through the Oversight Review step (step five) and determined that it took an average of 217 calendar days, with a range of 91 to 245 calendar days, to complete the step. The average number of calendar days the IRS took to complete the eight applications through the first four steps was 42 calendar days, with a range of 20 to 62 calendar days, and through the fifth step, an average of 175 calendar days, with a range of 32 to 218 calendar days. The reason so much time elapsed in the Oversight Review (step five) was that IRS executives first convened in February 2019 but did not begin reviewing applications for approval until April 2019, which was six months after the first public-facing application completed the Implementation Determination step. The eight public-facing applications were approved on June 4, 2019.

Other factors affecting the completion of the DIRA process included the preparation of IRS processes and systems due to the Tax Cuts and Jobs Act of 2017[8] for the 2019 Filing Season from October to December 2018; the loss of effort during the 35 calendar-day Government shutdown from December 22, 2018, to January 25, 2019; the 2019 Filing Season from January 2019 to May 2019 that needed increased oversight by IRS leadership because of the Tax Cuts and Jobs Act; and a 14 calendar-day lapse in the DIRA process contract support that expired on May 31, 2019, which led to the rescheduling of three public-facing applications. We anticipate similar conditions, *i.e.*, the upcoming preparation for and the 2020 Filing Season, which could impact the IRS achieving its January 2020 goal.

[7] The number of taxpayers who annually access the Get Transcript and Identity Protection Personal Identification applications are not unique. In addition, for the Get Transcript application taxpayer count, it could include multiple transcripts that a single taxpayer requested.
[8] Pub. L. No. 115-97, 131 Stat. 2054 (2017). Officially known as "An act to provide for reconciliation pursuant to titles II and V of the concurrent resolution on the budget for Fiscal Year 2018."

Recommendation

Recommendation 1**:** The Chief Information Officer should coordinate with the Business Unit Commissioners, as needed, and the Chief Privacy Officer to ensure that the remaining public-facing applications complete the first five steps in the DIRA process as scheduled to assist IRS compliance with NIST SP 800-63-3 guidelines for identity proofing.

> ***Management's Response:*** The IRS agreed with the recommendation. Based on funding and resource availability, the Cybersecurity office will coordinate with the Business Unit Commissioners and the Chief Privacy Officer to ensure that the remaining public-facing applications complete the first five steps in the DIRA process as scheduled to assist IRS compliance with NIST SP 800-63-3 guidelines for identity proofing.

A Digital Identity Proofing Solution Is Being Designed; However, Some Challenges Are Affecting Its Implementation

After NIST SP 800-63-3 guidelines were issued in June 2017, the Chief Information Officer tasked the Application Development's IAM function with developing a strategy to conform with these guidelines. The IAM function coordinated with its stakeholders to develop a modernized solution that would address the following key drivers:

- Securing taxpayer data.
- Meeting taxpayer expectations and modernizing technology and solutions.
- The evolving cybersecurity threat landscape.
- Identity proofing a customer base that interacts with the IRS for various personal and professional tax reasons, *i.e.*, to electronically file returns, to check refund status, and to make tax payments.
- Opportunities to support security first and to improve the taxpayers' experience.

The IAM function decided on the Secure Access Digital Identity (SADI) platform as its modernized solution. On June 24, 2018, the IAM function formed the Design and Innovation Branch, with the responsibility to design and deliver the SADI platform.

The Enterprise Services function developed the vision, scope, and architecture for the SADI platform with a goal to layout the conceptual architecture and then the logical architecture. Currently, the IRS has a conceptual vision, scope, and architecture. The vision includes empowering taxpayers to engage online with the IRS by providing a simpler and more secure front door for secure registration, identity proofing, and being compliant with NIST SP 800-63 guidelines within IRS context and providing a leading example for future iterations of Digital Identity Federal directives and standards. The scope includes accepting identity assertions and

credentials from trusted CSPs and having audit and logging services that will track end-to-end activity of both external users and internal administrators across the SADI platform. The architectural vision, using the Get Transcript application as an example, is as follows:

> *A taxpayer wants to log in. The taxpayer clicks Log In on the Get Transcript IRS site and would select a login option (e.g., login.gov). The taxpayer then goes through the process on login.gov, and is provided with a token through the web browser (nothing the taxpayer can actually see). That token then goes to the IRS when the taxpayer is sent back to the login, and it contains the information the IRS needs to determine what level the taxpayer has been approved for in terms of access.*

While the IRS has developed the concept for the SADI platform to include a focus on security and empowering taxpayers, the IRS faces the following challenges to deliver the modernized solution: 1) testing the solution to prove assumptions and to make further decisions, as needed; 2) operating with levels of assurance that are based on superseded NIST guidelines; 3) the CSPs with limitations; and 4) implementing requirements of the Office of Management and Budget memorandum.

Testing the modernized solution to prove assumptions and make further decisions

The Design and Innovation Branch plans to test its modernized solution in four phases, which will ultimately prove out the assumptions made when performing a series of analyses of alternatives to determine the optimal method to achieve the SADI vision. The first phase involves installing an enterprise infrastructure product, for testing only, that enables a centralized web access management system to enable user authentication and single sign-on, policy-based authorization, identity federation, and auditing of access to web applications. In essence, this product could provide flexibility to users by using one set of login credentials to allow access to multiple applications within the enterprise.

The IRS plans to perform this first phase between June 2019 and November 2019, and will make a decision about the outcome and plan to make any adjustments as needed. The next two phases are planned for October 2019 to January 2020 and December 2019 to May 2020. The final phase of the test, from June 2020 to November 2020, is a pilot with a CSP from end to end with one of the IRS's public-facing applications. Following the completion of the four tests, the IRS plans to complete a go/no-go evaluation of the platform based on the test results. In addition, the IRS plans to develop a plan to successfully migrate all of the online applications from the current system to the SADI platform by an undetermined implementation date.

Operating with levels of assurance that are based on superseded NIST guidelines

As we described earlier in this report, the IRS is operating with levels of assurance supported by the superseded NIST SP 800-63-2 guidelines for *2* of 25 **********2********** **********2**********. The levels of assurance are not comparable to the NIST SP 800-63-3

requirements for the applications designated as xAL2, which introduces the need for either remote or physically present identity proofing. We estimate that the ******2****** could have approximately 250 million user accesses each year, so better security is needed for the taxpayer data.

The remaining 38 applications are in varied risk-based assessment steps in the DIRA process and could receive the IAL2 designation, further adding to the number of applications with taxpayer data that need better security. Given the previously stated timeline for the tests, the decisions that will follow, and the unknown implementation date for the modernized solution, we are concerned about the length of time the IRS will be operating with the existing levels of assurance for the applications that taxpayers will access to accomplish online business. In addition, the length of time could be further extended because of preparation for and operation during the upcoming filing season, which is the period from January through mid-April, and is a critical time for the IRS.

CSP limitations

The current CSPs have limited access to identity information that can be used to identity proof taxpayers or tax professionals because it is either owned by the States, which are protective of their residents' information, or owned by other Federal identity credential issuers, such as the Department of State for passports and the Department of Defense for the military. IRS personnel stated that they were not planning to work directly with the 50 States to obtain access to identity data but will leverage external CSPs and their access to State data.

We met with personnel from two vendors, one in the private sector and the other in the Government sector, about their identity proofing solutions.[9] We asked each vendor to share how its proofing solution works as well as any thoughts and concerns they have with implementing NIST guidelines.

- The first vendor, Vendor A, stated it is IAL2 certified. The vendor received its certification from a nonprofit-based organization as a result of an audit, using a checklist containing the NIST guidelines. The vendor has access to approximately 52 percent of the States driver's license information via the American Association of Motor Vehicle Administrators. The vendor told us that each State's department of motor vehicle would corroborate the text information contained on the license. However, the States will neither share pictures nor biometric information, which are the strongest identity proof, from its issued licenses.
- The second vendor, Vendor B, stated that it is very close to IAL2 readiness and recently received its authorization to operate. However, the vendor does not believe that IAL2 is fully implementable due to remote access issues to the source data, *i.e.*, driver's license information and passport information, which are needed for IAL2-designated

[9] The IRS met with the two vendors in August 2019, which was after we completed our fieldwork.

applications. The vendor also uses the American Association of Motor Vehicle Administrators for driver's license information; however, it is working with the Department of State to get a verification check with passports. Vendor personnel cited accuracy concerns with the accrediting process and believed it is sound to have one organization perform the accrediting, but they cautioned that getting to full IAL2 is still challenging.

We examined the NIST guidelines to determine what tasks a CSP must perform to successfully identity proof an applicant who wants access to Government digital services or benefits. There are three phases – resolution, validation and verification – along with tasks for each phase that are to be completed for successfully identity proofing an applicant. Figure 4 outlines the phases and tasks.

Figure 4: NIST Guidelines for a CSP to Successfully Identity Proof Applicants

Resolution	Validation	Verification
1.a. The CSP collects Personally Identifiable Information from the applicant, *i.e.*, name, address, date of birth, e-mail, and telephone number.	2.a. The CSP validates the information supplied in 1.a by checking an authoritative source. The CSP determines that the information supplied by the applicant matches the authoritative source's records.	3.a. The CSP asks the applicant to take a photo of themselves, with liveness checks, to match the license and passport.
1.b. The CSP collects two forms of identity evidence, *i.e.*, a driver's license and a passport. For example, using the camera of a laptop, the CSP can capture a photo of both sides of both pieces of identity evidence.	2.b. The CSP checks the images of the license and the passport and determines that there are no alterations, that the encoded data matches the plain-text information, that the identification numbers follow standard formats, and that the physical and digital security features are valid.	3.b. The CSP matches the pictures on the license and the passport to the applicant picture and determines that they match.
	2.c. The CSP queries the issuing sources for the license and passport and validates the information matches.	3.c. The CSP sends an enrollment code to the validated telephone number of the applicant; the applicant provides the enrollment code to the CSP; and the CSP confirms they match, verifying that the applicant is in possession and control of the validated telephone number.
		3.d. The applicant has been successfully proofed.

Source: NIST SP 800-63A.

Given the phases previously outlined for the CSPs, the number of users who annually access the IAL2-designated applications, and the extensive amount of Personally Identifiable Information

that has been stolen because of breaches in the public and private sector, we are concerned with the IRS's ability to identity proof all taxpayers' identities when they use online services. The IRS stated that it is unable to cover everyone throughout the country and would have to perform demographic analyses to identify coverage gaps and how to expand its efforts to meet those gaps. Because of the expressed coverage limitations, we believe the IRS will need Federal Government as well as State Government assistance, through a CSP, for identity proofing its taxpayer and tax professional user population.

The Federal Government and the States are coordinating their efforts to improve the reliability and accuracy of State-issued identification documents through the REAL ID effort; however, the thrust for that effort is law enforcement related.[10] Identity proofing for access to IRS public-facing applications to accomplish online business is currently not considered to be law enforcement related. We reviewed the law that supports the REAL ID effort and noted that, if the provision below could be expanded to include Federal bureau electronic access, identity proofing for the IRS's IAL2 public-facing applications could be addressed.

> *Provide electronic access to all other States to information contained in the motor vehicle database of the State. Maintain a State motor vehicle database that contains, at a minimum—all data fields printed on drivers' licenses and identification cards issued by the State.*

Implementing requirements of the Office of Management and Budget memorandum

In May 2019, the Office of Management and Budget issued Memorandum M-19-17,[11] updating guidance to heads of executive departments and agencies for efficient operations to identify, credential, monitor, and manage users that access Federal resources. The memorandum includes responsibilities for designated agencies, *i.e.*, the Department of Commerce and the General Services Administration, to improve the management and use of digital identity. The Department of Commerce's responsibilities include publishing and maintaining, within six months, a roadmap with timelines and milestones to develop criteria for accrediting products and services. The General Services Administration's tasks include, within six months, developing and maintaining a roadmap to determine the feasibility, in coordination with the Office of Management and Budget, of establishing or leveraging a public or private sector capability for accrediting Identity, Credential, and Access Management products and services, and that the capability leverages NIST 800-63 assurance levels. The completion of these responsibilities was due in November 2019 and, even then, they will likely result in additional actions to be taken.

[10] The REAL ID Act, passed by Congress in 2005, Public Law 109–13, 119 Stat. 231, enacted the 9/11 Commission's recommendation that the Federal Government "set standards for the issuance of sources of identification, such as driver's licenses."

[11] Office of Management and Budget, Office of Management and Budget M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management* (May 2019).

When applying the memorandum to the SADI platform, the IRS believes the memorandum will not change its path forward but lessens the risk in selecting credentialed CSPs because of the designated agencies' involvement in properly accrediting the CSPs. We concluded that because the designated agencies will need to first determine the feasibility of establishing or leveraging public or private sector capabilities and issue further guidance, identifying the CSPs for agency consideration may not occur until a future time.

The IRS is aware of the challenges above and is carefully considering them as well as other security measures while developing SADI for identity proofing and authenticating taxpayers who want and need access to their data stored in IRS systems. However, it will not be a quick fix, and the IRS will continue to use compensating controls based on superseded NIST guidelines for the **********2********** that could have approximately 250 million user accesses annually to accomplish online business.

Recommendations

Recommendation 2**:** The Chief Information Officer should ensure that the IAM Design and Innovation Branch performs the planned tests; complete a go/no-go evaluation of the SADI platform based on the results from the tests; determine and incorporate the additional needs for the initial release of the SADI platform; and develop and implement the plan to successfully migrate all of the online applications from the current system of processes to the SADI platform, as expeditiously as is possible.

> ***Management's Response:*** The IRS agreed with the recommendation. The IAM Design and Innovation Branch is conducting a series of tests to validate the SADI solution. The results from these tests will be considered as part of the go/no-go evaluation and subsequent decision regarding the SADI platform. Based on the go/no-go decision, implementation plans to migrate all applications to the SADI platform and a follow-on planned corrective action will be created as needed.

Recommendation 3: The Deputy Commissioner for Operations Support should coordinate with the Department of the Treasury on legislative proposals or policy changes needed to obtain additional assistance from States, Territories, and Federal agencies that issue identifications in identity proofing users of the IRS's public-facing applications that require the IAL2.

> ***Management's Response:*** The IRS partially agreed with the recommendation. The IRS will provide the Department of the Treasury with a briefing paper on ways in which States, Territories, and Federal agencies that issue identifications could assist the IRS with identity proofing users of its public-facing applications that require IAL2 so that the Department of the Treasury may pursue legislative proposals or policy changes as appropriate.
>
> ***Office of Audit Comment:*** While the IRS partially agreed, we believe its planned corrective action meets the intent of our recommendation. We met with representatives

from the Department of the Treasury's Office of Tax Policy Office to provide information on this issue.

Generally, the Public-Facing Applications Generate Audit Logs, but Some Logs Did Not Include Administrators' Actions and Other Required Data

Internal Revenue Manual 10.8.1, *Information Technology Security, Policy and Guidance*,[12] provides guidance for implementing and managing security for information systems security within the IRS. Included in the guidelines are audit and accountability policy and procedures that outline what audit events information systems should capture, the content of the audit records from the systems, and that the systems should employ automated mechanisms to integrate audit review, analysis, and reporting processes to support investigation and a response to suspicious activities.

We reviewed information from the Systems Security Plans, TIGTA Office of Investigations' results from its analysis of the Security Audit and Analysis System, and audit log data from the 25 public-facing applications (if data were available for them) and found the following results.

- The IRS generated audit trails for 20 applications, of which **********2********** and five were designated as IAL1. The IRS did not generate audit trails for the remaining five applications, of which **********2********** and one as IAL1. Of these five applications, two applications are currently offline and not in use, one application is hosted externally to the IRS as a managed service, one application is not in operation, and the remaining application does not generate audit trails because it is managed under another application.
- 19 of the 20 applications are sending audit trails to the Security Audit and Analysis System, a solution tailored to perform analyses for unauthorized access violation detection and investigations. The IRS is working toward sending the audit trails for the remaining application to the tailored solution.
- 7 of the 19 application audit trails sent to the tailored solution were accurate or complete regarding content and 12 were deficient. For example, we found six applications were not providing records on accesses by database and systems administrators and one application was not providing all of the required data, such as the Internet Protocol addresses, or was not providing the data in the correct field, such as the tax period and user identification number.

[12] Internal Revenue Manual 10.8.1 (May 9, 2019).

While opportunities exist to improve the audit trails for the public-facing applications, we will not make recommendations in this report, but will include them in our ongoing audit of the IRS's unauthorized access audit trail program.[13]

[13] TIGTA, Audit No. 201920006, *Unauthorized Access Audit Trails Follow-up*, final report scheduled for issuance in April 2020.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to evaluate the IRS's identity proofing capabilities for secure electronic authentication to online applications. To accomplish our objective, we:

I. Determined whether the IRS effectively implemented NIST enrollment and identity proofing requirements for its online tools and applications.

   A. Identified and reviewed policies, procedures, and guidelines related to identity proofing.

   B. Interviewed IAM personnel within the Applications Development function to determine the IRS's status in implementing identity proofing for online applications.

   C. Interviewed Identity Assurance function personnel within the Privacy, Governmental Liaison, and Disclosure office to determine the office's involvement and status in implementing identity proofing within the IRS for online applications.

   D. Determined whether the IRS will achieve its goal of applying the DIRA process[1] to all 63 public-facing applications[2] by the end of Calendar Year 2019.

   E. Assessed the IRS's identity proofing implementation plan.

II. Determined the effect that the Office of Management and Budget memorandum[3] will have on the implementation of identity proofing requirements for its online tools and applications.

   A. Reviewed the Office of Management and Budget memorandum to determine the responsibilities of the various Federal agencies and any associated timelines with those responsibilities.

   B. Determined whether the IRS developed plans to execute the requirements of the memorandum.

[1] See Appendix VI for a glossary of terms.
[2] The IRS identified 64 public-facing applications; however, only 63 were scheduled for the DIRA process to date. Hereafter, we will only address the 63 applications.
[3] Office of Management and Budget, Office of Management and Budget M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management* (May 2019).

III. Determined whether the DIRA process meets NIST guidelines for identity proofing.

A. Identified the required elements of identify proofing within NIST SP 800-63-3[4] and SP 800-63A.

B. Evaluated the DIRA process against the required elements of identity proofing identified in NIST guidelines.

C. Reviewed the IRS public-facing applications that completed the DIRA process through steps four and five as of July 1, 2019.

1. Obtained and reviewed supporting documentation to determine whether the IRS completed all the required steps of the DIRA process and determined the length of time each application took to go through the process.

2. Determined whether the IRS has ensured the applications have the appropriate audit logs and that the logs are available for investigation as appropriate.

3. Determined whether the assessed IAL is appropriate for each application reviewed.

D. Identified the reasons for the delays in the DIRA Oversight Review step.

IV. Evaluated the IRS's assessment of identity proofing service options.

A. Determined the progress the IRS has made to initiate additional identity proofing tests.

B. Evaluated the progress the IRS has made to develop its SADI platform that will allow the IRS to apply identity proofing to all of its online applications.

Internal controls methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: the Information Technology organization's policies and procedures for performing the DIRA process and NIST SP 800 63-3 and SP 800-63A. We evaluated these controls by interviewing Information Technology organization and Identity Assurance function staff, reviewing the draft DIRA SOP and NIST guidelines, comparing the draft DIRA SOP to NIST guidelines, and reviewing the public-facing applications against the DIRA process.

[4] These guidelines describe the risk management processes for selecting appropriate digital identity services and the details for implementing identity assurance, authenticator assurance, and federation assurance levels based on risk. They also supersede NIST SP 800-63-2.

Appendix II

Major Contributors to This Report

Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Deborah Smallwood, Audit Manager
Michael Segall, Lead Auditor
Cindy Harris, Senior Auditor

Appendix III

Report Distribution List

Deputy Commissioner for Services and Enforcement
Commissioner, Small Business/Self-Employed Division
Commissioner, Tax Exempt and Government Entities Division
Commissioner, Wage and Investment Division
Chief Information Officer
Chief Privacy Officer
Deputy Chief Information Officer for Operations
Associate Chief Information Officer, Applications Development
Associate Chief Information Officer, Cybersecurity
Associate Chief Information Officer, Enterprise Services
Director, Identity and Access Management
Director, Identity Assurance
Director, Security Risk Management
Director, Enterprise Audit Management

Appendix IV

Outcome Measure

This appendix presents detailed information on the measurable impact that our recommended corrective actions will have on tax administration. This benefit will be incorporated into our Semiannual Report to Congress.

Type and Value of Outcome Measure:

- Taxpayer Privacy and Security – Potential; taxpayer or practitioner access to *****2***** **********2********** for identity proofing (see page 4).

Methodology Used to Measure the Reported Benefit:

We reviewed the initial DIRA reports for the 25 public-facing applications that completed the Implementation Determination step, which is part of a data-driven approach to identity assurance risk determinations for IRS public-facing applications. The NIST SP 800-63-3 issued digital identity guidelines for Federal agencies to perform a risk assessment of their online public-facing applications and assign one of three IALs – IAL1, IAL2, or IAL3 – to assist in deciding what identity evidence users need to present to get access to information through the applications. For IAL1, the user does not need to provide evidence to a real-life identity. For IAL2, the user needs to provide evidence that supports a real-world existence either remotely or in person. For IAL3, the user needs to provide evidence of a real-life existence in person. The IRS processed the 25 public-facing applications using the risk assessment approach from October 2, 2018, through July 1, 2019, and determined that *2* of the 25 **********2********** for taxpayers or practitioners to access and accomplish online business.

The IRS does not have a technology solution yet for users, taxpayers, and practitioners to provide real-life evidence remotely, although it is designing such a solution. IRS management anticipates piloting a solution with one application beginning in June 2020 but does not know when the solution will be applied to all the applications. In the interim, the IRS has compensating controls in place to secure the taxpayer data; however, the controls are based on NIST guidelines that were superseded by the NIST SP 800-63-3 guidelines. *******2******** **********2********** **********2**********.

Much of the information that the IRS uses to provide assurance of the taxpayers' identity may have been stolen from the Government and the private sector from the numerous hacks over the years from the Office of Personnel Management, credit bureaus, Internet portals, retailers, banks, and finance-related companies. In addition, the information could be on either or both the Internet's dark web and in the possession of cyberthieves. Because the IRS does not have the

technology solution in place to require the appropriate identity proofing and the date when it will be available is unknown, it is unable to confirm with a high level of confidence taxpayers' and practitioners' identities when they use online services and products to accomplish tax administration business. Taxpayer privacy and security of their tax information is at risk.

Appendix V

The Digital Identity Risk Assessment Standard Operating Procedures Compliance With the 10 National Institute of Standards and Technology Required Elements

Required Element	Description of the NIST Requirement	Is the NIST Requirement in the DIRA SOP?
1	Agencies shall assess the risk of the proofing, authentication, and federation errors separately to determine the required assurance level for each transaction. Each assurance level, IAL, authenticator assurance level and federation assurance level (if accepting or asserting a federated identity) shall be evaluated separately.	Yes
2	Agencies shall develop a Digital Identity Acceptance Statement in accordance with SP 800-53 IA-1 a.1. The Acceptance Statement shall include at a minimum: • Assessed xAL. • Implemented xAL. • Rationale, if the implemented xAL differs from the assessed xAL. • Comparability demonstration of compensating controls when the complete set of applicable SP 800-63 requirements are not implemented. • Rationale, if not accepting federated identities.	Yes
3	An agency relying party shall select, based on risk, the following individual assurance levels: IAL, authenticator assurance level, and federation assurance level.	Not Applicable
4	Agencies shall assess the potential risks and identify measures to minimize their impact to determine the appropriate level of assurance of the user's asserted identity.	Yes

Required Element	Description of the NIST Requirement	Is the NIST Requirement in the DIRA SOP?
5	Agencies shall demonstrate comparability of any chosen alternative, to include any compensating controls, when the complete set of applicable SP 800-63 requirements is not implemented.	Yes[1]
6	Agencies shall not alter the assessed xAL based on agency capabilities.	Yes
7	Agencies shall implement procedures to document both the justification for any departure from normative requirements and detail the compensating control(s) employed.	Yes
8	As these guidelines are revised, the CSPs shall consider how changes in requirements affect their user population. This shall be a risk-based decision made in context of the CSP, any relying parties that use the CSP, the mission, and the population served.	Not Applicable
9	In analyzing risks, agencies shall consider all of the expected direct and indirect results of an authentication failure, including the possibility that there will be more than one failure or harms to more than one person or organization.	Yes
10	A value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification. For the purposes of these guidelines, key requirements shall meet the minimum requirements stated in Table 2 of NIST SP 800-57 Part 1.	Not Applicable

Source: NIST SP 800-63-3.

[1] TIGTA did not test the effectiveness of the IRS's compensating controls as we noted reference to them in the procedures. However, we evaluated the applicability of the controls to the current NIST requirement and concluded the controls are based on the superseded NIST SP 800-63-2 guidelines.

Appendix VI

Glossary of Terms

Term	Definition
American Association of Motor Vehicle Administrators	A tax-exempt, nonprofit organization developing model programs in motor vehicle administration, law enforcement, and highway safety. The association also serves as an information clearinghouse in these areas and acts as the international spokesman for these interests.
Applicant	An individual who opts to be identity-proofed by a CSP.
Audit Trails	A chronological record of system activities that is sufficient to permit reconstruction, review, and examination of a transaction from inception to final results.
Authenticator Assurance Level	A category describing the strength of the authentication process.
Biometrics	Security technologies that use a person's unique features, such as fingerprints, face or retina, and iris patterns, as a method of identification.
Botnet Attacks	A type of malicious attack that utilizes a series of connected computers to attack or take down a network, network device, website, or information technology environment.
Business Unit	A title for major IRS organizations such as the Office of Appeals, the Wage and Investment Division, the Office of Professional Responsibility, and the Information Technology organization.
Credential	An object or data structure that authoritatively binds an identity – via an identifier or identifiers and (optionally) additional attributes – to at least one authenticator possessed and controlled by a subscriber.
Credential Service Provider	A trusted entity that issues or registers subscriber authenticators and issues electronic credentials to subscribers. A CSP may be an independent third party or may issue credentials for its own use.
Cryptographic Operations	The execution of procedures to protect information and communications through the use of codes among computer systems, smartphones, and applications so that only those for whom the information is intended can read and process it.
Cybersecurity	A function within the IRS Information Technology organization responsible for ensuring compliance with Federal statutory, legislative, and regulatory requirements governing confidentiality, integrity, and availability of IRS electronic systems, services, and data.

Term	Definition
Digital Identity Risk Assessment Process	A redesign of the IRS's previous Electronic Authentication Risk Assessment process. This process identifies the risks to system security and determines the probability of occurrence, the resulting impact, and additional safeguards that would mitigate the impact.
Digital Identity Risk Assessment Results	A document that provides a record of all the data collected in the DIRA tool for an application.
Eavesdropping Attack	An attack in which an attacker listens passively to the authentication protocol to capture information that can be used in a subsequent active attack to masquerade as the claimant.
Federation Assurance Level	A category describing the assertion protocol used by the federation to communicate authentication and attribute information, if applicable, to a relying party.
Filing Season	The period from January through mid-April when most individual income tax returns are filed.
Fiscal Year	Any yearly accounting period, regardless of its relationship to a calendar year. The Federal Government's fiscal year begins on October 1 and ends on September 30.
Get Transcript Application	This application allows taxpayers to view and download their tax information, such as account transactions, line-by-line tax return information, and income reported to the IRS. Taxpayers can download or print five distinct transcript types: tax account, tax return, record of account, wage and income, and verification of nonfiling.
Identity and Access Management Function	Provides direction for all development activities for external authentication and authorization as well as technical integration and coordination of other public-facing applications in support of the Information Technology organization's secure data access activities, both within the IRS and with other Government agencies.
Identity Assurance Function	Provides IRS-wide policy leadership through collaborative decision-making, supporting, and coordinating the efforts of operating units to develop and integrate authentication, authorization, and access policy including related frameworks and processes.
Liveness Checks	A security feature that can ensure that biological identifiers are from the proper user and not from someone else. Traditional forms of detections can include eye or lip movement analysis, prompted motion instructions, texture/reflection detection in video feeds, or zooming motion detection.
Login.gov	A service that offers secure and private online access to Government programs, such as Federal benefits, services, and applications. With a login.gov account, users can sign in to multiple Government websites with the same e-mail address and password.

Term	Definition
Man-in-the-Middle Attack	An attack in which an attacker is positioned between two communicating parties in order to intercept and/or alter data traveling between them. In the context of authentication, the attacker would be positioned between claimant and verifier, between registrant and the CSP during enrollment, or between subscriber and the CSP during authenticator binding.
Network	An open communications medium, typically the Internet, used to transport messages between the claimant and other parties. Unless otherwise stated, no assumptions are made about the network's security; it is assumed to be open and subject to active (*e.g.*, impersonation, man-in-the-middle, session hijacking) and passive (*e.g.*, eavesdropping) attack at any point between the parties (*e.g.*, claimant, verifier, CSP, relying party).
Normative	Is based on what is considered to be the usual or correct way of doing something. For NIST guidelines, normative is used when presenting mandatory requirements.
Open Network	A wireless network that is unsecured and can be used by anyone in the vicinity.
Personally Identifiable Information	Information that can be used to distinguish or trace an individual's identity, such as his or her name, Social Security Number, and biometric records, alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date, place of birth, and mother's maiden name.
Relying Party	An entity that relies upon the subscriber's authenticator(s) and credentials or a verifier's assertion of a claimant's identity, typically to process a transaction or grant access to information or a system.
Remote	An information exchange between network-connected devices where the information cannot be reliably protected end to end by a single organization's security controls.
Security Audit and Analysis System	This system implements a data warehousing solution to provide online analytical processing of audit trail data.
Self-asserted	Any attribute or ascribed quality or characteristic provided by an applicant that has not been verified.
Session Hijacking Attack	An attack in which the attacker is able to insert himself or herself between a claimant and a verifier subsequent to a successful authentication exchange between the latter two parties. The attacker is able to pose as a subscriber to the verifier or vice versa to control session data exchange.
Subscriber	A party who has received a credential or authenticator from a CSP. If the applicant is successfully proofed, the individual is then termed a subscriber of that CSP.

Appendix VII

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

CHIEF INFORMATION OFFICER

FEB 28 2020

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy A. Sieger
Acting Chief Information Officer

SUBJECT: Response to Draft Audit Report - While Progress Is Being Made on Digital Identity Requirements, Completion Dates to Achieve Compliance With Identity Proofing Standards Have Not Been Established (audit #201920004)

Thank you for the opportunity to review your draft audit report and address the report observations with the audit team. The IRS is committed to the protection of taxpayer data and complying with the NIST Special Publication (SP) 800-63-3 guidelines. We continue to rely on a strong ID Proofing solution already in place as well as robust cybersecurity measures to help prevent the loss of federal tax data, protect federal revenues and significantly improve the security of online taxpayer services.

We are encouraged by the report's acknowledgement of the progress IRS is making toward implementing the NIST identity proofing guidelines. We share TIGTA's perspective regarding the level of risk inherent in providing service through internet-accessible public-facing applications. The IRS is in the process of creating a Secure Access Digital Identity (SADI) solution to meet the new guidelines; and using a test and learn approach to prove that the technology implementation will meet these new guidelines, while keeping the taxpayer experience in mind.

Pursuant to the NIST SP 800-63-3 guidelines, we use a risk-based decision-making process to determine the appropriate response on a system-by-system basis. The DIRA process is now a foundational requirement for our risk assessment and implementation of digital services. We are using the DIRA process to assess all public-facing applications and transactions to determine the appropriate identity and authentication assurance levels in accordance with the new NIST guidelines. (Note that the terms 'application' and 'transaction' are used synonymously in the report. For the DIRA process, IRS' web-applications are deconstructed into 63 smaller transactional elements to ensure we identify the appropriate requirements for each individual transactional capability for a given web-application.) Our goal is to bring all public-facing applications into compliance with the updated NIST guidelines by leveraging the SADI solution.

However, the speed at which we can migrate these applications will be dependent upon the ever-changing threat landscape and advances in available technology solutions that meet the stringent NIST guidelines.

We have made significant progress conducting the DIRA process against the 63 applications identified in the report. In fact, at the release of the Draft Audit Report, 70% of the identified applications have fully completed the DIRA process and the remainder have completed the first three phases and are on track to complete the DIRA process in 2020.

We agree with recommendations one and two and partially agree with recommendation three. Our corrective action plan for the recommendations identified in the report are attached.

The IRS values your continued support and the assistance your organization provides. If you have any questions, please contact me at (202) 317-5000 or a member of your staff may contact Patrice Wilmot, Director Identity Access Management, (240) 613-5270.

Attachment

Attachment

Corrective Action Plan

Draft Audit Report – While Progress is Being Made on Digital Identity Requirements, Completion Dates to Achieve Compliance With Identity Proofing Standards Have Not Been Established (audit #201920004)

RECOMMENDATION #1: The Chief Information Officer should coordinate with the Business Unit Commissioners, as needed, and the Chief, Privacy Officer to ensure that the remaining public-facing applications complete the first five steps in the DIRA process as scheduled to assist IRS compliance with NIST SP 800-63-3 guidelines for identity proofing.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. Based on funding and resource availability, Cybersecurity will coordinate with the Business Unit Commissioners and the Chief Privacy Officer to ensure that the remaining public-facing applications complete the first five steps in the DIRA process as scheduled to assist IRS compliance with NIST SP 800-63-3 guidelines for identity proofing.

IMPLEMENTATION DATE : June 15, 2020

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #2: The Chief Information Officer should ensure that the IAM Design and Innovation Branch performs the planned tests; complete a go/no-go evaluation of the SADI platform based on the results from the tests; determine and incorporate the additional needs for the initial release of the SADI platform; and develop and implement the plan to successfully migrate all of the online applications from the current system of processes to the SADI platform, as expeditiously as is possible.

CORRECTIVE ACTION #2a: The IRS agrees with this recommendation. The IAM Design and Innovation Branch is currently conducting a series of tests to validate the SADI solution. The results from these tests will be considered as part of the go/no-go evaluation and subsequent decision regarding the SADI platform.

IMPLEMENTATION DATE : September 15, 2021

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Applications Development

CORRECTIVE ACTION #2b: The IRS agrees with this recommendation. Based on the results of the tests of the SADI solution, a go/no-go decision will be made. Implementation plans to migrate all applications to the SADI platform and develop a follow-on Planned Corrective Action (PCA) will be created as needed.

IMPLEMENTATION DATE : February 15, 2022

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Applications Development

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into JAMES and monitor them on a monthly basis until completion.

RECOMMENDATION #3: The Deputy Commissioner for Operations Support should coordinate with the Department of the Treasury on legislative proposals or policy changes needed to obtain additional assistance from States, Territories, and Federal agencies that issue identifications in identity proofing users of the IRS's public-facing applications that require the IAL2.

CORRECTIVE ACTION #3: IRS partially agrees with this recommendation. The IRS will provide the Department of the Treasury a briefing paper on ways in which States, Territories, and Federal agencies that issue identifications could assist the IRS with identity proofing users of its public-facing applications that require IAL2 so that Treasury may pursue legislative proposals or policy changes as appropriate.

IMPLEMENTATION DATE : September 30, 2020

RESPONSIBLE OFFICIALS: Director, Identity Assurance

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into JAMES and monitor them on a monthly basis until completion.