United States Government Accountability Office

Report to Congressional Requesters

May 2019

DATA PROTECTION

Federal Agencies Need to Strengthen Online Identity Verification Processes

Accessible Version

GAO-19-288

May 2019

DATA PROTECTION

Federal Agencies Need to Strengthen Online Identity Verification Processes

GAO Highlights

Highlights of GAO-19-288, a report to congressional committees

Why GAO Did This Study

Many federal agencies rely on CRAs, such as Equifax, to help conduct remote identity proofing. The 2017 breach of data at Equifax raised concerns about federal agencies' remote identity proofing processes.

GAO was asked to review federal agencies' remote identity proofing practices in light of the recent Equifax breach and the potential for fraud. The objectives of this review were to (1) describe federal practices for remote identity proofing and the risks associated with those practices, (2) assess federal agencies' actions to ensure the effectiveness of agencies' remote identity proofing processes, and (3) assess the sufficiency of federal identity proofing guidance.

To do so, GAO identified remote identity proofing practices used by six agencies (CMS, GSA, IRS, SSA, USPS, and VA) with major, public-facing web applications providing public access to benefits or services. GAO compared the agencies' practices to NIST's remote identity proofing guidance to assess their effectiveness, and compared NIST's and OMB's guidance to requirements in federal law and best practices in IT management to assess the sufficiency of the guidance.

View GAO-19-288. For more information, contact Nick Marinos at (202) 512-9342 or MarinosN@gao.gov, or Michael Clements at (202) 512-8678 or ClementsM@gao.gov.

What GAO Found

Remote identity proofing is the process federal agencies and other entities use to verify that the individuals who apply online for benefits and services are who they claim to be. To perform remote identity proofing, agencies that GAO reviewed rely on consumer reporting agencies (CRAs) to conduct a procedure known as knowledge-based verification. This type of verification involves asking applicants seeking federal benefits or services personal questions derived from information found in their credit files, with the assumption that only the true owner of the identity would know the answers. If the applicant responds correctly, their identity is considered to be verified. For example, the Social Security Administration (SSA) uses this technique to verify the identities of individuals seeking access to the "My Social Security" service, which allows them to check the status of benefit applications, request a replacement Social Security or Medicare card, and request other services.

However, data stolen in recent breaches, such as the 2017 Equifax breach, could be used fraudulently to respond to knowledge-based verification questions. The risk that an attacker could obtain and use an individual's personal information to answer knowledge-based verification questions and impersonate that individual led the National Institute of Standards and Technology (NIST) to issue guidance in 2017 that effectively prohibits agencies from using knowledge-based verification for sensitive applications. Alternative methods are available that provide stronger security, as shown in Figure 1. However, these methods may have limitations in cost, convenience, and technological maturity, and they may not be viable for all segments of the public.

Figure 1: Examples of Alternative Identity Verification and Validation Methods that Federal Agencies Have Reported Using

Remote assessment of physical credentials

Modern technology can allow an individual to use their cellphone to capture an image of a physical credential (e.g. driver's license), which can be compared to the documentation on file to confirm authenticity of the credential.

Verification of mobile device possession

A verifying entity can query records maintained by the various cell phone carriers to verify the identity of an individual who is in possession of a specific phone and number.

Source: GAO analysis based on agency data. | GAO-19-288

What GAO Recommends

GAO is making recommendations to six agencies to strengthen online identify verification processes:

- GAO recommends that CMS, SSA, USPS, and VA develop plans to strengthen their remote identity proofing processes by discontinuing knowledge-based verification.
- GAO recommends that NIST supplement its technical guidance with implementation guidance to assist agencies in adopting more secure remote identity proofing processes.
- GAO recommends that OMB issue guidance requiring federal agencies to report on their progress in adopting secure identity proofing practices.

Four agencies—Commerce (on behalf of NIST), SSA, USPS, and VA—agreed with GAO's recommendations. These agencies outlined the additional steps they plan to take to improve the security of their remote identity proofing processes. One agency, HHS (on behalf of CMS), disagreed with GAO's recommendation because it did not believe that the available alternatives to knowledge-based verification were feasible for the individuals it serves. However, a variety of alternative methods exist, and GAO continues to believe CMS should develop a plan for discontinuing the use of knowledge-based verification. OMB provided a technical comment, which GAO incorporated, but OMB did not provide any comments on GAO's recommendation.

Two of the six agencies that GAO reviewed have eliminated knowledge-based verification. Specifically, the General Services Administration (GSA) and the Internal Revenue Service (IRS) recently developed and began using alternative methods for remote identity proofing for their Login.gov and Get Transcript services that do not rely on knowledge-based verification. One agency—the Department of Veterans Affairs (VA)—has implemented alternative methods for part of its identity proofing process but still relies on knowledge-based verification for some individuals. SSA and the United States Postal Service (USPS) intend to reduce or eliminate their use of knowledge-based verification sometime in the future but do not yet have specific plans for doing so. The Centers for Medicare and Medicaid Services (CMS) has no plans to reduce or eliminate knowledge-based verification for remote identity proofing.

Several officials cited reasons for not adopting alternative methods, including high costs and implementation challenges for certain segments of the public. For example, mobile device verification may not always be viable because not all applicants possess mobile devices that can be used to verify their identities. Nevertheless, until these agencies take steps to eliminate their use of knowledge-based verification, the individuals they serve will remain at increased risk of identity fraud.

NIST has issued guidance to agencies related to identity proofing and OMB has drafted identity management guidance, but their guidance is not sufficient to ensure agencies are adopting such methods. Sound practices in information technology (IT) management state that organizations should provide clear direction on how to implement IT objectives. However, NIST's guidance does not provide direction to agencies on how to successfully implement alternative identity-proofing methods with currently available technologies for all segments of the public. For example, the guidance does not discuss the advantages and limitations of currently available technologies or make recommendations to agencies on which technologies should be adopted. Further, most of the agencies that GAO reviewed reported that they were not able to implement the guidance because of limitations in available technologies for implementing alternative identify proofing methods. NIST officials stated that they believe their guidance is comprehensive, and at the time of our review they did not plan to issue supplemental implementation guidance to assist agencies.

The *Federal Information Security Modernization Act of 2014 (*FISMA) requires that OMB oversee federal agencies' information security practices. Although OMB has the authority under this statute to issue guidance, OMB has not issued guidance requiring agencies to report on their progress in implementing NIST's identity proofing guidance. OMB staff plan to issue guidance on identity management at federal agencies, but their proposed guidance does not require agencies to report on their progress in implementing NIST guidance. Until NIST provides additional guidance to help agencies move away from knowledge-based verification methods and OMB requires agencies to report on their progress, federal agencies will likely continue to struggle to strengthen their identify proofing processes.

Contents

Figures

Abbreviations

CMS	Centers for Medicare and Medicaid Services
CRA	consumer reporting agency
DOD	Department of Defense
GSA	General Services Administration
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PII	personally identifiable information
PIN	personal identification number
SMS	short message service
SSA	Social Security Administration
USPS	United States Postal Service
VA	Department of Veterans Affairs

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

May 17, 2019

Congressional Requesters

In recent years, the risk of fraud has increased as significant amounts of personally identifiable information (PII) have been compromised by large-scale cyberattacks. Such attacks have been widespread—impacting federal agencies as well as retailers, hospitals, insurance companies, consumer reporting agencies (CRA), and other large organizations. For example, in June and July 2015, the Office of Personnel Management (OPM) announced that it had detected two data breaches affecting approximately 22.1 million current or former federal employees, contractors, and their family members. Further, in 2017, the consumer reporting agency, Equifax, announced that a breach of its online consumer dispute portal had resulted in the compromise of records containing the PII of at least 145.5 million individuals in the United States.

The PII stolen during such cyberattacks can be used to commit identity fraud for financial or other gain. The Equifax breach, in particular, raised concerns about the vulnerability of federal agencies that rely on information maintained by CRAs to verify the identity of individuals who apply electronically for benefits and services. Among others, the customers of Equifax's services included federal agencies such as the Internal Revenue Service (IRS); Social Security Administration (SSA); and U.S. Postal Service (USPS).

The process of using an online exchange of information to verify that an individual is who he or she claims to be is known as remote identity proofing. Federal agencies and other entities often rely on the information provided by CRAs to perform remote identity proofing of individuals who are applying for benefits and services. The Office of Management and Budget (OMB) is developing policy guidance on identity management and the National Institute of Standards and Technology (NIST) has issued technical guidance on identity proofing.

In response to your request, we issued a report on the July 2017 Equifax data breach in August 2018.[1] The report noted that hackers had accessed

[1]GAO, *Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach,* GAO-18-559 (Washington, DC: Aug. 30, 2018).

people's names, Social Security numbers, birth dates, addresses, and, in some instances, driver's license numbers. While there was no breach of federal systems or information, agencies sought to determine which of their customers were directly affected by the breach, recognizing that those individuals could be at heightened risk of identity fraud. We reported that agency officials had expressed concern about how the breached data could be used to compromise sensitive information or fraudulently procure government services, even from agencies that are not direct customers of Equifax.[2]

You also asked us to review federal programs that rely on CRAs for remote identity proofing. In conducting this review, our specific objectives were to (1) describe selected federal agency practices for remote identity proofing of individuals seeking access to major web-based applications using services provided by consumer reporting agencies and the risks associated with those practices; (2) assess selected federal agencies' actions to ensure the effectiveness of agencies' remote identity proofing processes; and (3) assess the sufficiency of federal identity proofing guidance developed by OMB and NIST in assuring the security of federal systems.

To address the first objective, we made a non-probability selection of federal agencies with major public-facing web applications that use identity proofing solutions provided by the three nationwide CRAs (Equifax, Experian, and TransUnion). We considered "major" applications to be those that could involve interaction with millions of individuals across the entire country. We selected six agencies to review: the Centers for Medicare and Medicaid Services (CMS), General Services Administration (GSA), IRS, SSA, USPS, and the Department of Veterans Affairs (VA).

In addition, we reviewed federal identity proofing guidance to obtain detailed information about remote identity proofing concepts and practices. We also interviewed relevant officials at NIST to understand the current federal digital identity guidelines and obtain their views on the risks associated with commonly-used remote identity proofing processes. Further, we interviewed officials responsible for the identity proofing

[2]We also reviewed federal oversight of CRAs and consumer rights regarding the protection of PII collected by CRAs. See GAO, *Consumer Data Protection: Actions Needed to Strengthen Oversight of Consumer Reporting Agencies*, GAO-19-196 (Washington, DC: Feb. 21, 2019).

programs at the six selected agencies and at ID.me, a commercial provider that offers identity proofing solutions to federal agencies and other entities, to obtain information about identity proofing techniques used to verify remote users of electronic applications. Other than the three nationwide CRAs, ID.me was the only commercial provider of identity proofing solutions used by the agencies selected for this review.

To address the second objective, we compared documentation of the remote identity proofing processes used at the six selected agencies with federal requirements specified in NIST's technical guidance on remote identity proofing.[3] We also interviewed officials at the selected agencies to obtain information on what plans, if any, they have to improve the security of their remote identity proofing processes in light of the Equifax data breach and the potential for similar breaches in the future.

To address the third objective, we compared NIST's guidance on remote identity proofing to best practices in IT governance for providing clear and sufficient guidance.[4] We also interviewed officials at the selected federal agencies who managed access to major web applications using remote identity proofing about whether the NIST guidance provided sufficient direction to assist them in implementing appropriate remote identity proofing methods. In addition, we interviewed relevant NIST officials to discuss the effectiveness of the existing remote identity proofing guidance.

Further, we reviewed OMB's draft policy that, when issued, is expected to direct agencies to implement NIST's guidance for their remote identity proofing processes. We compared OMB's draft policy to the *Federal Information Security Modernization Act of 2014*'s (FISMA) requirements for OMB to oversee agencies' implementation of information security policies. We assessed whether OMB's draft policy included requirements that would allow OMB to monitor agencies' progress in implementing NIST's remote identity proofing guidance. In addition, we interviewed OMB staff regarding their plans to finalize the draft policy. Appendix I discusses our objectives, scope, and methodology in greater detail.

[3]NIST, *Digital Identity Guidelines*, Special Publication 800-63-3; and *Digital Identity Guidelines: Enrollment and Identity Proofing*, Special Publication 800-63A (June 2017).

[4]ISACA, *Control Objectives for Information and Related Technology* (COBIT)® 2019, ©2018.

We conducted this performance audit from November 2017 to May 2019 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Individuals engage in countless online transactions every day—from checking their bank accounts and making retail purchases to signing up for federal benefits and services. However, securing such transactions is a complex endeavor. A key part of this process is verifying that the person who is attempting to interact for the first time with an organization, such as a federal agency or a business, is the individual he or she claims to be. This process, known as identity proofing, is essential to prevent fraud, which could cause harm to both individuals and organizations.[5]

Identity proofing may occur in person or through a remote, online process. In the case of in-person identity proofing, a trained professional verifies an individual's identity by making a direct physical comparison of the individual's physical features and other evidence (such as a driver's license or other credential) with official records to verify the individual's identity. Verification of these credentials can be performed by checking electronic records in tandem with physical inspection. In-person identity proofing is considered a strong method of identity proofing.

However, it may not always be feasible to require that all applicants appear in person. In such cases, remote identity proofing is performed. Remote identity proofing is the process of conducting identity proofing entirely through an online exchange of information. When remote identity proofing is used, there is no way to confirm an individual's identity through their physical presence. Instead, the individual provides the information electronically, or performs other electronically verifiable actions that

[5]While an individual may be able to simply assert an identity for certain types of interactions, like registering for notification of an event or other publicly available information, many federal services require greater assurance of an applicant's identity. Some examples of federal services that need stronger identity proofing include applying for Medicare or Social Security benefits, filing an income tax return, and changing postal address information.

demonstrate his or her identity. Because many federal benefits and services are offered broadly to large numbers of geographically dispersed applicants, agencies often rely on remote identity proofing to verify the identities of applicants.

Overview of the Remote Identity Proofing Process

Remote identity proofing involves two major steps: (1) resolution and (2) validation and verification. During the resolution step, an organization determines which specific identity an applicant is claiming when they first attempt to initiate a transaction, such as enrolling for federal benefits or services, remotely. The most common form of remote interaction is through an organization's website. The organization starts the identity resolution process by having the applicant provide identifying information, typically through a web-based application form. Examples of information that an organization may collect for identity resolution include name, address, date of birth, and Social Security number.

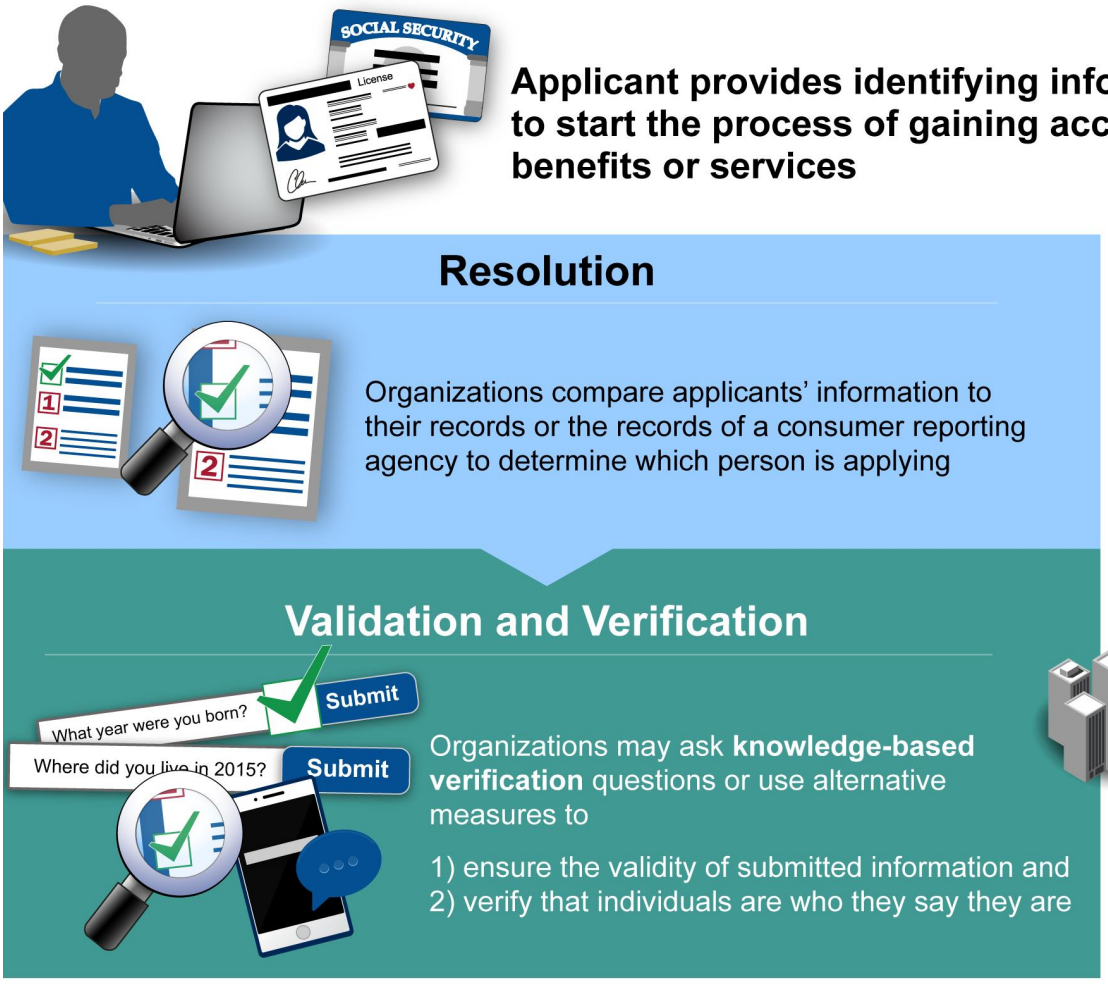
The organization then electronically compares the applicant's identifying information with electronic records that it already has in its databases or with records maintained by another entity, such as a CRA, to determine (or "resolve") which identity is being claimed. For example, if an individual named John Smith were applying, the organization would obtain enough identifying information about him to determine which "John Smith" he is from among the thousands of John Smiths that it may have in its records or that may be documented in the records of the CRA that it is using for this process.

Once the resolution process is complete, the process of validation and verification occurs. In this process, steps are taken to verify whether the applicant is really who they claim to be. For example, in the case of John Smith, it is not enough simply to determine which John Smith is being claimed, because the claimant may not really be John Smith at all. Organizations need to obtain electronic evidence from the remote applicant to verify their identity. Organizations can use a variety of techniques to accomplish this goal. Knowledge-based verification is a technique that commonly has been used for this purpose.

With knowledge-based verification, organizations ask applicants detailed and personal questions, under the presumption that only the real person will know the answers to these questions. To do this, the organization poses a series of multiple choice questions through an online web form,

and the applicant selects the appropriate responses and submits the answers through the web form. If the applicant has chosen the correct responses, through the remotely accessed web form, their identity is considered to be verified, and the validation and verification step is complete. Figure 1 depicts the typical process that organizations use for remote identity proofing (including the use of knowledge-based verification).

Figure 1: Typical Steps in the Remote Identity Proofing Process



Source: GAO analysis of National Institute of Standards and Technology guidance. | GAO-19-288

The Role of CRAs in Knowledge-Based Verification

As previously mentioned, to perform knowledge-based verification for remote identity-proofing, federal agencies and other organizations often use services provided by CRAs. The CRAs assemble and evaluate consumer credit and other information from a wide variety of sources. Equifax, Experian, and TransUnion—the three nationwide CRAs—use the personal information they obtain about individuals from organizations, such as financial institutions, utilities, cell phone service providers, public records, and government sources, to compile credit files containing detailed records about individuals. They then use the information in these files to offer a variety of services to federal agencies and other entities. These services can include identity verification, as well as verification of income and employment of a candidate for a job or an applicant for benefits or services.

To support organizations that rely on knowledge-based verification, CRAs generate multiple choice questions that organizations can use to test applicants' knowledge of information in their credit files. The organizations using the CRA services do not generate the questions themselves, because they do not have access to the credit history information maintained by the CRAs. Rather, the CRAs' remote identity proofing systems transmit the questions and multiple choice answers to the organization through an automated electronic connection with the organization's website. The organization's website then displays the questions and multiple choice answers to the applicant through the web application that the applicant is using to apply for access to benefits or services.

Typically, the questions generated by CRA identity proofing systems ask about lenders, mortgage details, current and past home addresses, or credit card accounts. Once the applicant has selected answers to the questions and enters them in the online application, the organization's automated system electronically relays the applicant's responses to the CRA's remote identity proofing system; this system then compares the responses with information in the applicant's credit file. If this comparison determines that the applicant correctly responded to the questions, then the applicant's identity is considered to be verified.[6] The CRA's identity

[6]The organizations using CRA identity verification services can tailor the knowledge-based verification process by specifying the number of questions to be asked and how many must be answered correctly for the verification process to be considered successful.

proofing system electronically transmits the results of its comparison to the organization's website to allow the applicant, whose identity is now considered verified, to proceed with applying for benefits or services.

OMB and NIST Provide Guidance to Agencies on Information Security Management

The *Federal Information Security Modernization Act of 2014* (FISMA) is intended to provide a comprehensive framework for ensuring the effectiveness of security controls over information resources that support federal operations and assets, as well as the effective oversight of information security risks.[7] FISMA assigns responsibility to the head of each agency to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information systems used or operated by an agency or on behalf of an agency.

FISMA assigns responsibility to NIST for developing comprehensive information security standards and guidelines for federal agencies. These include standards for categorizing information and information systems according to ranges of risk levels and guidelines for establishing minimum security requirements for federal information systems.[8]

To fulfill its FISMA responsibilities, NIST has issued technical guidance on many different aspects of information security, including identity proofing. NIST issued its first guidance related to identity proofing in 2011.[9] In 2017, NIST released an updated version of its guidance, which included guidance on identity proofing that outlines technical requirements for resolving, validating, and verifying an identity based on

[7]The *Federal Information Security Modernization Act of 2014* (Pub. L. No. 113-283, Dec. 18, 2014) largely superseded the *Federal Information Security Management Act of 2002* (FISMA 2002), enacted as *Title III, E-Government Act of 2002*, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers to the new requirements in FISMA 2014, and to other relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

[8]NIST issues technical guidance to assist agencies in implementing their FISMA responsibilities and policies set by OMB.

[9]NIST, *Electronic Authentication Guideline*, Special Publication 800-63-1 (December 2011).

evidence obtained from a remote applicant.[10] OMB requires agencies to implement NIST's technical guidance on information security subjects within one year of issuance. In the case of NIST's updated guidelines for remote identity proofing, agencies would have needed to implement the guidance by June 2018 to meet OMB's time frames.

FISMA assigns responsibility to OMB for overseeing agencies' information security policies and practices. OMB, in turn, has established requirements for federal information security programs and has assigned agency responsibilities to fulfill the requirements of statutes such as FISMA. OMB policies and guidance require agencies to employ a risk-based approach and decision making to ensure that security and privacy capabilities are sufficient to protect agency assets, operations, and individuals.

OMB has not issued guidance to agencies specifically on identity proofing. However, OMB developed a draft policy document in April 2018 that is intended to provide guidance to agencies on strengthening the security of information and information systems to ensure safe and secure access to federal benefits and services.[11] While it has not yet been issued, the draft policy indicates that OMB intends to provide policy-level guidance for agencies to identify, credential, monitor, and manage user access to information and information systems and adopt sound processes for authentication and access control.

Selected Agencies Use a Variety of Remote Identity Proofing Techniques, Including Knowledge-Based Verification

The six agencies that we reviewed rely on a variety of remote identity proofing techniques, including knowledge-based verification, to ensure that the individuals who enroll for federal benefits and services are who they claim to be. These agencies typically use knowledge-based verification services offered by CRAs, which generate questions for the

[10]NIST, *Digital Identity Guidelines*, Special Publication 800-63-3; and *Digital Identity Guidelines: Enrollment and Identity Proofing*, Special Publication 800-63A (June 2017).

[11]Office of Management and Budget, *Strengthening the Cybersecurity of Federal Agencies through Improved Identity, Credential, and Access Management (Draft)*, April 6, 2018, Washington, D.C.

individuals applying for benefits or services and check the applicants' answers to verify their identity. However, to the extent that they use knowledge-based verification, these agencies face risks because an attacker could obtain and use an individual's personal information to answer knowledge-based verification questions and successfully impersonate that individual.

Centers for Medicare and Medicaid Services

CMS oversees several federal health insurance programs, including the Medicare and Medicaid programs, which provide health insurance coverage. CMS is also responsible for administering the federal health insurance marketplace established under the *Affordable Care Act*, known as Healthcare.gov. Through this marketplace, individuals may apply for health coverage programs, such as Medicaid, which CMS jointly administers with the states. Individuals may also use Healthcare.gov to apply for private health insurance coverage, known as qualified health plans, for which individuals may qualify for federal income-based financial subsidies.

CMS uses knowledge-based verification to remotely verify individuals' identities prior to granting them access to its Healthcare.gov service. In this regard, CMS collects the names, dates of birth, and addresses provided by applicants to determine their identities. It then collects from the applicants answers to questions related to their personal and financial information, as generated by a CRA's remote identity proofing service. CMS electronically relays the answers provided by applicants to the CRA, which then scores the responses. Applicants who answer the questions accurately are allowed to establish an account on Healthcare.gov. Applicants who cannot successfully complete the remote, knowledge-based verification process are directed to submit information by mail for manual review and verification.

General Services Administration

GSA provides a variety of information technology and other mission-support services to agencies across the federal government. One service that it offers is Login.gov, which is intended to provide a consolidated web portal for agencies to use in securing government online interactions.[12]

[12]GSA collaborates with OMB's U.S. Digital Service to provide Login.gov.

Specifically, for agencies that use Login.gov, the service acts as the publicly accessible website that verifies the identities of individuals seeking access to a particular agency's benefits or services. Login.gov is intended to allow such individuals access to multiple government agency programs securely and privately with one email address and password. As of April 2019, Login.gov was being used by a variety of agency programs, including OPM's USAJOBS.gov application, the Department of Homeland Security's Trusted Traveler Program, and GSA's System for Award Management, among others.[13]

Login.gov guides each individual through a multi-step process to verify their identity before they are allowed to access the specific online agency application they are seeking. First, the individual is asked to use their cell phone to provide an image of a government-issued identification card, such as a driver's license, which GSA compares with information it obtains from the American Association of Motor Vehicle Administrators or another third-party source. The individual next submits a phone number, which GSA verifies through a CRA or another third-party that checks phone company records to determine whether the phone number belongs to the individual. GSA then confirms possession of that phone number by sending a one-time PIN via a text message or voice call that the individual enters into the Login.gov application. For individuals who cannot be verified this way, Login.gov attempts to confirm the individual's street address by sending a one-time PIN via postal mail.

At the time of our review, GSA's Login.gov service did not provide in-person identity-proofing services as a backup if any of these methods failed. In the event that an individual was unable to be verified through Login.gov, the agency whose services the individual was trying to access was required to provide a backup process, such as an in-person process, to verify the individual's identity. However, according to GSA officials responsible for Login.gov, GSA is working with USPS to develop a process to perform in-person identity proofing at USPS retail locations.

[13]USAJOBS.gov is the federal government's official employment site and connects job seekers with federal employment opportunities. The Trusted Traveler Program is managed by the Department of Homeland Security and allows international travelers to apply for expedited entry into the United States. The System for Award Management is used by contractors to register to do business with the U.S. government, update or renew business entity registration, check the status of an entity registration, and search for entity registration and exclusion records.

Internal Revenue Service

As the nation's tax collection agency, IRS provides a variety of online services to help taxpayers understand and meet their tax responsibilities. The agency relies on online interactions with citizens to file taxes, provide information on prior year returns, and provide other services that taxpayers may require. For example, "Get Transcript" is an online application that provides users the ability to view, print, and download tax returns and account transcripts; download wage and income documents; and generate other tax records.

IRS guides each individual through a series of steps to verify their identity before they are allowed access to the services available on Get Transcript. Specifically, the individual submits a phone number, which IRS verifies through a CRA that checks phone company records to determine whether the phone number belongs to the individual. IRS then confirms possession of that phone number by sending a one-time PIN via a text message. The individual then enters the PIN into the Get Transcript application. For individuals who cannot be verified this way, IRS attempts to confirm the individual's street address by sending the confirmation PIN via postal mail.

Social Security Administration

SSA administers social programs covering disability, retirement, and survivors' benefits. SSA developed an online system called "My Social Security," which allows individuals to request a replacement Social Security or Medicare card, check the status of benefit applications, access Social Security statements, and obtain benefit verification letters.

SSA uses knowledge-based verification to remotely verify the identity of each individual seeking access to the "My Social Security" service. Through the "My Social Security" website, the agency asks these individuals to provide identifying information (e.g., Social Security number, date of birth, and mailing address) and to respond to knowledge-based verification questions generated by a CRA. SSA's system electronically relays the individuals' responses to the CRA's identity proofing system. The CRA system then electronically compares the answers to information in the CRA's records and transmits an electronic response to the SSA "My Social Security" website as to whether the individual responded correctly to the questions.

SSA determines how many questions are to be asked and how many correct responses are required for an applicant's identity to be considered successfully verified. If enough of the questions have been answered correctly based on the threshold determined by SSA, the individual's identity is considered to be verified. SSA allows individuals to choose in-person identity proofing if they cannot or choose not to complete the online process.

United States Postal Service

USPS is responsible for delivering billions of pieces of mail each year to about 156 million delivery points across the United States. USPS offers online access to various services associated with mail delivery, including change of address requests and a service known as "Informed Delivery," which allows individuals to digitally preview letter-sized mail and manage incoming packages. Currently, over 13 million users have signed up for Informed Delivery and more than 40 million Americans change their addresses annually, including by submitting online requests through the USPS Change of Address service.

USPS uses knowledge-based verification to verify the identity of individuals seeking online access to its Informed Delivery service. Specifically, the Informed Delivery service prompts an individual to provide responses via its online website to knowledge-based verification questions generated by a CRA or by another third-party provider of identity verification services. The Informed Delivery system then electronically relays the individual's responses to the CRA's system and the third party's system. The CRA and the third-party service provider electronically compare the answers provided by the individual to information in their records and transmit an electronic response to the Informed Delivery website as to whether the individual responded correctly to the questions.

USPS determines how many questions are to be asked and how many correct responses are required for an applicant's identity to be considered successfully verified. If enough of the questions have been answered correctly based on the threshold determined by USPS, the individual's identity is considered to be verified.

While USPS does not use knowledge-based verification for its online Change of Address service, it uses a third-party service provider that contracts with a CRA to verify the identity of individuals seeking to change their mailing address online. Specifically, the agency verifies the address

associated with the credit card that the individual uses to pay for the online Change of Address service with the third-party service provider to ensure the address matches either the old or new address being provided by the individual. USPS officials stated that individuals who do not have a credit card or fail the online process may visit a USPS retail location to complete the change-of-address process. According to USPS officials, the agency plans to expand its in-person identity proofing capabilities to include most post offices and postal carriers in fiscal year 2019.

Department of Veterans Affairs

VA provides a wide range of health services and benefits to approximately 9 million veterans and their family members, including medical care, education benefits, insurance, home loan services, and disability compensation benefits. VA allows service members and veterans to apply for benefits using the agency's MyHealtheVet, VA.gov, and eBenefits systems. These web portals provide resources and self-service capabilities to veterans, service members, and their families to research, access, and manage their VA and military benefits and personal information.

VA uses knowledge-based verification to verify the identity of individuals seeking online access to its services. The agency relies on two different methods for remote identity proofing. Specifically, for individuals applying for certain benefits who may be affiliated with the Department of Defense (DOD), it uses DS Logon, an online identity management service run by DOD that relies on a CRA to generate knowledge-based questions as part of its remote identity proofing process. For other applicants, VA uses a commercial identity verification service that combines knowledge-based and other methods, such as verifying photos of documents submitted by individuals, to remotely verify an identity.

As an alternative to remote identity proofing using DS Logon, the agency allows individuals to choose in-person identity proofing at a regional VA office or by telephone through VA's National Call Center. If they choose in-person identity proofing, individuals are required to provide government-issued photo identification that includes a name and date of birth that matches the information provided in the enrollment application. Individuals that wish to use the telephone identity proofing option must be in receipt of benefits through direct deposit.

Knowledge-Based Verification Poses Risks, but Alternative Techniques Have Been Developed That Are More Secure

Although commonly used by federal agencies for remote identity proofing, knowledge-based verification techniques pose security risks because an attacker could obtain and use an individual's personal information to answer knowledge-based verification questions and successfully impersonate that individual. As such, NIST's 2017 guidance on remote identity proofing effectively prohibits the use of knowledge-based verification for sensitive applications.[14] The guidance states that the ease with which an attacker can discover the answers to many knowledge-based questions and the relatively small number of possible responses cause the method to have an unacceptably high risk of being successfully compromised by an attacker.[15] In its guidance, NIST states that the agency no longer recommends using knowledge-based verification because it tends to be error-prone and can be frustrating for users, given the limitations of human memory.

According to NIST officials, private-sector providers of remote identity proofing solutions and officials at the agencies we reviewed, alternative methods for verifying an individual's identity are available that are not knowledge-based and can provide stronger security assurance than knowledge-based verification. Specific examples of such techniques include:

- **Remote assessment of physical credentials.** Recently developed technology allows an agency to remotely examine a physical credential, such as a driver's license or a passport, to verify an individual's identity. For example, an agency may have the individual use their mobile device, such as a cell phone, to capture and submit an image of their driver's license to an agency or commercial provider of identity proofing services. The agency or commercial provider can then compare the image to documentation on file to confirm the authenticity of the credential. Technological advances in how images are captured and processed by mobile devices, such as cell phones,

[14]The guidance allows the use of knowledge-based verification only for a small part of the identity proofing process and only when strong evidence of a claimed identity is not required.

[15]NIST Special Publication 800-63A.

can provide improved assurance that the photos transmitted by these devices are genuine and that the credentials are authentic.

- **Verification of mobile device possession.** Many individuals use their cell phones on a near-continuous basis and keep their phones with them. These actions create a record of the owner's connection with these mobile devices that is difficult for an imposter to falsify.

  Accordingly, an organization can query records maintained by cell phone carriers to verify the identity of an individual who is in possession of a specific mobile device and phone number. By doing this, the organization can determine how long the individual has had that particular device, compare unique identifiers, and determine if the location matches the individual's billing information. The organization can be confident that the individual legitimately possesses the device if the device has been in use for some time and its current location corresponds to one where the device has been known to be used by its owner. Since an individual's location information is obtained directly from the device and compared with cell phone carrier records, data entry errors by the individual, such as mistyping a phone number, are minimized and the risk of impersonation is reduced.

- **Verification through mobile device confirmation codes.** An additional method that organizations use to help verify an individual's identity is to verify that an individual possesses a telephone number that they have supplied as part of the remote identity proofing process. Organizations perform verification of an individual's possession of a phone number by sending a code to that phone number through the short message service (SMS) or another protocol, and ask the individual to enter the code into the online identity proofing application.[16] This process can provide additional assurance about the individual's identity because the verification code is transmitted through a separate electronic channel (specifically, the telephone system) from the online application where the remote identity proofing process was initiated.

  However, unlike the process for verifying the possession of a mobile device, the use of these codes may not prevent an imposter from using a stolen phone or stolen phone number. An imposter may be able to successfully complete the identity verification process if the

[16]Short message service (SMS) is a text messaging service component of most telephone, internet, and mobile-device systems. It uses standardized communication protocols to enable mobile devices to exchange short text messages.

applicant's possession of the physical device has not been independently verified. In its remote identity proofing guidance, NIST requires federal agencies to use confirmation codes as a supplement to other identity proofing measures.[17]

- **Verification through postal mail confirmation codes.** Another method that organizations use to help verify an individual's identity is to send a confirmation code, such as a personal identification number (PIN), through the mail system to the individual's address of record. The individual then enters the PIN in the organization's online application to confirm that they received the code in the mail. Like the use of mobile device confirmation codes, the use of postal mail codes can provide additional assurance about the individual's identity because the code is sent through a separate medium from the online application where the remote identity proofing process was initiated.

Even with these alternatives to knowledge-based verification, however, there are limitations to the security assurances that can be provided. One way to overcome these security limitations is for a trained professional to conduct identity proofing in person. This is generally considered to be a strong approach because it allows for direct physical comparison of an individual's documentation, including photographic evidence, to the individual attempting to enroll. Verification of the credentials being submitted can be performed by checking electronic records in tandem with physical inspection.

Figure 2 provides examples of alternative identity verification and validation methods that federal agencies have reported using.

[17]NIST Special Publication 800-63A.

Figure 2: Examples of Alternative Identity Verification and Validation Methods that Federal Agencies Have Reported Using

Remote assessment of physical credentials

Modern technology can allow an individual to use their cellphone to capture an image of a physical credential (e.g. driver's license), which can be compared to the documentation on file to confirm authenticity of the credential.

Verification of mobile device possession

A verifying entity can query records maintained by the various cell phone carriers to verify the identity of an individual who is in possession of a specific phone and number.

In-person identity proofing

The best way to overcome the limitations of remote identity proofing solutions is for a trained professional to conduct identity proofing in person. This is generally considered to be a strong approach because it allows for direct physical comparison of an individual's documentation, including photographic evidence, to the individual attempting to enroll.

Source: GAO analysis based on agency data. | GAO-19-288

Each of the alternatives to knowledge-based verification has other limitations, including implementation challenges. For example, in-person identity proofing is expensive to implement because it requires organizations to staff and maintain offices or other physical access points in multiple locations, and it can be inconvenient for applicants because it

requires travel to one of these locations. Mobile device verification may not always be viable because not all applicants possess a mobile device that can be used to verify their identity. In addition, fraudsters can manipulate or "spoof" phone numbers that redirect phone calls and SMS confirmation codes to an attacker. Sending confirmation codes by postal mail can result in a delay in an individual being able to gain access to the services or benefits he or she is seeking.

Several of the Selected Agencies Have Taken Steps to Better Ensure the Effectiveness of Their Remote Identity Proofing Processes, but Only Two Have Eliminated the Use of Knowledge-Based Verification

As previously discussed, in 2017, NIST released an updated version of its technical guidance on remote identity proofing.[18] NIST's 2017 guidance effectively prohibits the use of knowledge-based verification for sensitive applications because of the security risks associated with this technique.

For applications where identity verification is important, the guidance prohibits agencies from providing access to online applications based solely on correct responses to knowledge-based questions. Rather, the guidance provides detailed specifications regarding the required features of the identity evidence (such as driver's licenses and birth certificates) that an individual is to provide and how agencies are to verify that evidence. Agencies are restricted to using knowledge-based verification only for the very limited role of linking a single piece of identity evidence to an individual and only for applications where the identity verification process is not of critical importance. As a result, agencies are effectively prohibited from using traditional knowledge-based questions—the type of questions typically used in identity verification services provided by CRAs—as part of their processes. Thus, in order for agencies to ensure the effectiveness of their remote identity proofing processes, they are required to find ways to eliminate the use of knowledge-based verification.

[18]NIST Special Publication 800-63A.

Three of the six agencies we reviewed—GSA, IRS, and VA—have taken steps to enhance the effectiveness of their remote identity proofing processes. GSA and IRS recently eliminated knowledge-based verification from their Login.gov and Get Transcript services, respectively. VA has implemented alternative methods, but only as a supplement to the continued use of knowledge-based verification.

Among the other three agencies, two of them–SSA and USPS–are investigating alternative methods and have stated that they intend to reduce or eliminate their use of knowledge-based verification sometime in the future; however, these agencies do not yet have specific plans for doing so. One other agency, CMS, has no plans to reduce or eliminate knowledge-based verification for remote identity proofing.

General Services Administration Eliminated Knowledge-Based Verification from its Login.gov Service and Is Implementing Additional Verification Techniques

GSA has implemented alternative methods to knowledge-based verification for Login.gov. While GSA used knowledge-based verification on its Login.gov service in the past, the agency has recently implemented alternative verification techniques that do not rely on knowledge-based verification.

Specifically, GSA conducts independent verification of an applicant's possession of a mobile device, an alternative technique we previously discussed. GSA contracts with a third-party vendor to compare status information about the phone number provided by an individual with telephone company records to confirm the individual's identity. Further, GSA officials responsible for Login.gov stated that they plan to include additional alternative verification methods to Login.gov in the near future. Specifically, by the end of May 2019, the agency plans to implement software capable of analyzing and validating photos of documentation, such as driver's licenses, provided by applicants to further enhance the verification of their identities. In 2018, the agency tested this technology through a pilot program.

GSA officials responsible for Login.gov stated that they are pursuing several other initiatives to further enhance the verification techniques they use for Login.gov. For example, they are researching new software methods for confirming the authenticity of face images and other biometric information that could be transmitted by applicants to confirm

their identity. According to the officials, additional work is needed to ensure that a fraudulent image, such as a photo of a mask, is not being provided in lieu of a live image—a threat known as a "presentation attack."

The GSA officials also said they would like to work with other federal agencies to leverage data that have already been verified, such as USPS-validated mailing addresses, passport and visa information maintained by the Department of State, and IRS tax data. However, the officials cited legal and regulatory restrictions to sharing agency data as a challenge to being able to make use of resources such as these.

GSA's recent elimination of knowledge-based verification from its Login.gov identity proofing process is consistent with NIST's 2017 guidance on remote identity proofing and reduces the risk of fraud associated with using Login.gov. The additional enhancements and coordination that the agency is working on, if successful, will likely further improve the effectiveness of its remote identity proofing processes.

Internal Revenue Service Eliminated Knowledge-Based Verification and Is Examining Additional Verification Techniques

IRS has implemented alternative methods to knowledge-based verification for Get Transcript. While IRS used knowledge-based verification on its Get Transcript service in the past, the agency has recently implemented alternative verification techniques that do not rely on knowledge-based verification.

Specifically, IRS conducts independent verification of an applicant's possession of a mobile device and uses mobile device confirmation codes, alternative techniques we previously discussed. IRS contracts with a CRA to compare status information about the phone number provided by an individual with telephone company records to confirm the individual's identity. Further, IRS officials responsible for Get Transcript's identity proofing and authentication services stated that they plan to continue to add alternative verification methods to Get Transcript in the future. They stated that, in June 2017, in response to the release of NIST's updated digital identity proofing requirements, the agency started a task force to examine the updated requirements and make recommendations on possible changes to IRS's processes to meet the updated guidance. According to the officials, the task force developed a

digital identity risk assessment process that the agency started using to assess external facing online transactions in October 2018.

IRS's recent elimination of knowledge-based verification from its Get Transcript identity proofing process and the additional enhancements that the agency is working on, if successful, will likely further improve the effectiveness of its remote identity proofing processes.

Department of Veterans Affairs Has Implemented Some Alternative Methods, but Has No Plans to Reduce or Eliminate its Remaining Use of Knowledge-Based Verification

VA has taken steps to better ensure the effectiveness of its remote identity proofing processes, but it continues to rely on knowledge-based verification for certain categories of individuals. As previously mentioned, VA relies on two different providers, a commercial identity verification service (called ID.me) and DOD's DS Logon, to conduct identity proofing for its benefits systems. These providers use a mix of knowledge-based verification and alternative techniques. DOD's DS Logon verifies applicants using knowledge-based verification, while the commercial provider uses both knowledge-based verification processes as well as stronger alternative techniques. For example, the commercial provider uses cellular phone data to verify an applicant's identity based on the device subscriber's relationship to a claimed identity and the subscriber's tenure with the carrier.

VA's commercial provider can also remotely authenticate identity documents. In this regard, applicants can scan the front and back of driver's licenses, state identification, and passports, and upload the images to the commercial provider, which then analyzes the images to ensure that the documents meet standards and contain valid information. Further, the provider verifies applicants by having them take photos of themselves and then using facial recognition technology to match the applicants' images with their identity documents.

VA officials in the agency's information technology and benefits program offices believe that the alternative forms of identity proofing used by its commercial provider as a supplement to knowledge-based verification provide an acceptable level of assurance. Nevertheless, the officials acknowledged that it is important to eventually eliminate knowledge-based verification from the agency's identity-proofing processes.

However, the agency does not have specific plans with time frames and milestones to eliminate the use of knowledge-based verification. VA officials stated that it has not yet established plans for doing so because of its reliance on DOD's DS Logon service, which still uses knowledge-based verification. Until it develops a specific plan with time frames and milestones to eliminate its reliance on knowledge-based verification, VA and the individuals it serves will continue to face a degree of identity fraud risk that could be reduced.

Social Security Administration Intends to Eliminate Knowledge-Based Verification, but Does Not Yet Have Specific Plans for Doing So

SSA continues to rely on knowledge-based verification for its My Social Security service, but SSA officials stated that the agency intends to eliminate knowledge-based verification in the future. According to the SSA Chief Information Security Officer, in fiscal year 2019, the agency intends to pilot alternative verification methods, such as using the commercial ID.me service. In addition, the official said SSA plans to research other alternatives that could be used to replace knowledge-based verification, including modernizing its legacy systems so that they can use Login.gov or another shared identity management platform. The agency has set a goal of eliminating the use of knowledge-based verification in fiscal year 2020.

As an interim measure to reduce the risks associated with knowledge-based verification, SSA officials stated that they limit the period of time and the number of attempts that an individual has to answer the knowledge-based verification questions. These limitations are designed to prevent a potential fraudster from researching the answers to the questions. In addition, SSA also sends a confirmation code via email or SMS, which individuals must enter online before being given access to their account.

SSA does not yet have specific plans and milestones to achieve its goal of implementing enhanced remote identity proofing processes by fiscal year 2020. SSA officials stated that they cannot develop specific plans until they are able to identify an alternative method or methods that can be used successfully by all members of the public with which the agency interacts. Until SSA develops specific solutions for eliminating knowledge-based verification, the agency and the individuals that rely on its services will remain at an increased risk of identity fraud.

United States Postal Service Intends to Eliminate Its Use of Knowledge-Based Verification, but Does Not Yet Have Complete Plans and Time frames for Doing So

USPS has not yet fully implemented alternative methods to better ensure the effectiveness of its remote identity proofing processes. According to officials responsible for the agency's identity proofing program, USPS mitigates the risk of using knowledge-based verification by sending a written confirmation to the physical address associated with each identity-proofing transaction and provides instructions for what to do if the transaction is unauthorized or fraudulent.

In addition to this mitigation measure, the officials reported that they regularly evaluate new capabilities to further increase confidence in their identity-proofing processes and are planning several additional measures to supplement the use of knowledge-based verification. Specifically, in September 2018, USPS began allowing customers to request a confirmation code via the mail to allow them to enroll in Informed Delivery. In addition, the agency is planning on implementing verification of mobile device possession and SMS enrollment code verification in 2019 and other techniques at a subsequent time. According to USPS officials, these alternative techniques are expected to reduce the agency's use of knowledge-based verification. The officials said that USPS has not completely eliminated the use of knowledge-based verification because available alternatives to the agency's current processes do not satisfactorily address critical factors that they consider when deciding whether to implement alternative processes. These factors include cost, projected ability to reduce fraud and protect consumers, projected extent of the population that could be covered, and the burden on customers to complete the process.

The officials stated that the agency intends to implement alternative methods in the future for its Informed Delivery service but does not yet have specific plans with time frames and milestones. The officials noted that part of the reason for the slow implementation of alternative methods is that NIST technical guidance does not provide direction on how alternative methods are to be implemented and that additional guidance from NIST would be helpful to the agency for developing and

implementing a plan to eliminate knowledge-based verification for the Informed Delivery service.[19]

While the supplemental processes implemented by USPS to date may help to reduce the risks associated with using knowledge-based verification, they do not eliminate such risks. Until it completes a plan with time frames and milestones to eliminate its reliance on knowledge-based verification for Informed Delivery, USPS and its customers will remain at increased risk of identity fraud.

Centers for Medicare and Medicaid Services Has No Plans to Reduce or Eliminate its Use of Knowledge-Based Verification

CMS has not implemented alternative methods to better ensure the effectiveness of the remote identity proofing processes used for its Healthcare.gov service. CMS officials in the Office of Information Technology and the Office of Consumer Information and Insurance Oversight stated that the agency uses a two-step email verification process to reduce the risks associated with knowledge-based verification. Specifically, individuals applying for an account on Healthcare.gov provide basic information (e.g., name, email address, password) and then are asked to acknowledge an email confirmation they receive from CMS. The email confirmation is intended to prove that the individual applying for a Healthcare.gov account is in possession of the email address that same individual provided to CMS.

However, this process confirms only the email address that was used to create the account; it does not confirm the identity of the individual who is applying for the account. CMS stated that it uses this process because other mitigating measures are not cost effective. However, NIST's guidance does not permit agencies to use knowledge-based verification on the basis of cost effectiveness. Further, the agency does not have specific plans with time frames or milestones to eliminate its use of knowledge-based verification for Healthcare.gov.

[19]In August 2018, the USPS Office of Inspector General evaluated USPS' identity verification controls for its Change of Address service. The report recommended that USPS implement a national policy to require individuals to present government-issued identification when submitting hard copy change of address forms. It also recommended that USPS make changes to its online Change of Address identity verification processes.

CMS officials acknowledge that they do not have a plan to reduce or eliminate the use of knowledge-based verification because they have not yet identified any effective alternatives to knowledge-based verification for Healthcare.gov. According to these officials, based on a user study they conducted, individuals who use the agency's services prefer knowledge-based verification over any available alternatives. In addition, the officials stated that certain alternatives, such as mobile device verification, may not always be suitable for the population they serve. As one example, not all applicants have a mobile device that could be used to remotely verify the individual's identity. The CMS officials noted that NIST technical guidance does not provide direction on how alternative methods are to be implemented, given that they may not always be suitable for the population served by Healthcare.gov. However, until CMS takes steps to develop a plan with time frames and milestones to eliminate the use of knowledge-based verification, CMS and Healthcare.gov applicants will remain at an increased risk of identity fraud.

NIST and OMB Have Not Provided Sufficient Guidance to Ensure Agencies Move to More Secure Forms of Remote Identity Proofing

While NIST has issued guidance to agencies related to identity proofing and OMB is drafting identity management guidance, these efforts are not sufficient to ensure that agencies adopt secure methods for remote identity proofing. As previously discussed, NIST's guidance effectively prohibits the use of knowledge-based verification during the validation and verification phases of the remote identity proofing process, but does not provide direction to agencies on how to successfully implement alternative methods for remote identity proofing for large and diverse segments of the population.[20] Further, OMB has not issued guidance requiring agencies to report on their implementation of remote identity proofing processes, which is essential for monitoring agencies' progress.

[20]NIST Special Publication 800-63A.

NIST Guidance Does Not Provide Sufficient Direction to Agencies on How to Implement Alternative Methods for Remote Identity Proofing

Best practices in IT management state that organizations should provide clear direction in order to achieve objectives. Specifically, the *Control Objectives for Information and Related Technologies* (COBIT), a framework of best practices for IT governance, states that organizations should provide clear direction for IT projects, including relevant and usable guidance, and ensure that those implementing the technology have a clear understanding of what needs to be delivered and how.[21]

However, NIST has not issued any supplemental implementation guidance to its 2017 technical guidance to ensure that agencies have a clear understanding of what needs to be done to implement alternative methods of remote identity proofing, as called for in the technical guidance. For example, NIST's technical guidance provides abstract descriptions of identity evidence that individuals must provide, such as a credential containing a photograph or other biometric identifier as well as anti-counterfeiting security features. The guidance states that such credentials can be provided in person or remotely but does not detail the processes needed for providing credentials remotely.

For example, the guidance does not discuss the advantages and limitations of currently available technologies that agencies could successfully use to remotely verify credentials provided by individuals or to make recommendations to agencies on which technologies should be adopted. As previously discussed, several potential limitations could make choosing an alternative method difficult. Technologies such as secure, remote verification of a physical credential may not be commercially available. Also, some alternative technologies require that individuals use cell phones and maintain a verifiable record of having them in their possession. The NIST guidance does not discuss how agencies should accommodate segments of the public who do not possess advanced technological devices, such as cell phones, that may be needed for successful remote verification. Because the guidance does not include specific advice or direction on implementing alternative

[21]ISACA, *Control Objectives for Information and Related Technology* (COBIT)® 2019. ©2018.

technologies, agencies may be unable to determine what alternative methods are viable for the populations they serve.

As previously discussed, several of the agencies we reviewed send confirmation codes to applicants via cell phone, email, or postal mail, as ways that they believe compensate for risks associated with using knowledge-based verification. However, NIST officials do not consider such methods for remote verification to be effective in compensating for the risks associated with knowledge-based verification. Instead, the NIST technical guidance requires agencies to send confirmation codes by mail when they use any remote identity proofing method, including more advanced, alternative verification methods, such as verification of mobile device possession.

Officials from CMS, SSA, and USPS stated that they have not eliminated their use of knowledge-based verification in part because the existing NIST technical guidance does not provide direction on how alternative methods are to be implemented, given the various limitations of those alternative methods that agencies have identified. The officials stated that federal agencies could benefit from additional guidance on implementing the alternative verification techniques called for in the NIST technical guidance.

In response to these agencies' comments about being unable to fully implement the remote identity proofing guidance, NIST officials stated that agencies were expected to use their own judgment to determine how to meet the remote identity proofing requirements. The officials added that it was NIST's position that the updated guidance was comprehensive enough for agencies to follow. Thus, at the time of our review, NIST did not have plans to assist agencies by issuing implementation guidance to supplement its existing technical guidance. NIST officials stated that they are available to provide assistance on an individual basis to agencies that seek their advice.

Without additional guidance from NIST on how agencies are to implement the alternative identity proofing methods specified in an agency's existing technical guidance, agencies may not be using the most effective and secure identity-proofing methods, thus exposing their systems to risk of fraud.

OMB Guidance Does Not Include Reporting Requirements to Facilitate Monitoring of Agencies' Implementation of Secure Remote Identity Proofing

FISMA requires the Director of OMB to oversee agency information security policies and practices. However, OMB has not provided agencies with guidance establishing reporting requirements for OMB to use in monitoring agencies' progress in implementing secure remote identity proofing processes. For example, OMB has not proposed including reporting requirements for remote identity proofing in its draft policy on identity, credential, and access management, nor has it included reporting requirements in its FISMA reporting guidance to agencies for fiscal year 2019.[22]

According to OMB staff, OMB plans to issue guidance to agencies on the implementation of identity, credential, and access management. OMB issued a draft of this guidance for public comment in April 2018.[23] However, the draft guidance does not include a requirement for agencies to report on progress in implementing secure remote identity proofing processes.

Because it does not require agency reporting on progress in implementing secure remote identity proofing processes, OMB does not have visibility into the extent that agencies rely on insecure methods, particularly knowledge-based verification. Without establishing effective oversight measures, OMB cannot adequately monitor agency progress in implementing the secure identity proofing methods called for in NIST's 2017 technical guidance. As a result, agencies may be at risk of implementing weak methods of remote identity-proofing for individuals who seek access to services and benefits from the federal government, which may put both the federal government and individuals at risk for fraud.

[22]OMB, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*, Memorandum M-19-02 (Oct. 25, 2018).

[23]OMB, *Strengthening the Cybersecurity of Federal Agencies through Improved Identity, Credential, and Access Management*, (Apr. 6, 2018).

Conclusions

The six agencies that we reviewed rely on a variety of remote identity proofing techniques to help ensure that the individuals who enroll for federal benefits and services are who they claim to be. Several of the selected agencies use knowledge-based verification processes that rely on CRAs to pose questions to individuals and check their answers as a way of verifying their identities before granting them enrollment in a federal benefit or service. However, given recent breaches of sensitive personal information, these agencies face risks because fraudsters may be able to obtain and use an individual's personal information to answer knowledge-based verification questions and successfully impersonate that individual to fraudulently obtain federal benefits and services.

Two agencies we reviewed, GSA and IRS, recently implemented remote identity proofing processes for Login.gov and Get Transcript that allow individuals to enroll online without relying on knowledge-based verification. However, four agencies (CMS, SSA, USPS, and VA) were still using knowledge-based verification to conduct remote identity proofing. Moreover, none of the four agencies have developed specific plans to eliminate knowledge-based methods from their processes. Without such plans, these federal agencies and the individuals that rely on such processes will remain at risk for identity fraud.

NIST has issued technical guidance regarding remote identity proofing, but it may not be sufficient to help ensure that federal agencies adopt more secure methods. NIST's guidance does not provide direction on how agencies can adopt more secure alternatives to knowledge-based verification while also addressing issues of technical feasibility and usability for all members of the public. In addition, OMB has not issued guidance setting agency reporting requirements that OMB could use to track implementation of more secure processes across the federal government. Without additional guidance, federal agencies are likely to continue to rely on risky knowledge-based verification that could be used to fraudulently gain access to federal benefit programs and services.

Recommendations for Executive Action

We are making a total of 6 recommendations to CMS, NIST, OMB, SSA, USPS, and VA. Specifically:

The Administrator of the Centers for Medicare and Medicaid Services should develop a plan with time frames and milestones to discontinue knowledge-based verification, such as by using Login.gov or other alternative verification techniques. (Recommendation 1)

The Director of the National Institute of Standards and Technology should supplement the agency's 2017 technical guidance with additional guidance to assist federal agencies in determining and implementing alternatives to knowledge-based verification that are most suitable for their applications. (Recommendation 2)

The Director of the Office of Management and Budget should issue guidance requiring federal agencies to report on their progress in adopting secure identity proofing processes. (Recommendation 3)

The Commissioner of Social Security should develop a plan with specific milestones to discontinue knowledge-based verification, such as by using Login.gov or other alternative verification techniques. (Recommendation 4)

The Postmaster General of the United States should complete a plan with time frames and milestones to discontinue knowledge-based verification, such as by using Login.gov or other alternative verification techniques. (Recommendation 5)

The Secretary of the Department of Veterans Affairs should develop a plan with time frames and milestones to discontinue knowledge-based verification, such as by using Login.gov or other alternative verification techniques. (Recommendation 6)

Agency Comments and Our Evaluation

We requested comments on a draft of this report from the eight agencies included in our review. In response, we received written comments from six agencies—Commerce (on behalf of NIST), HHS (on behalf of CMS), IRS, SSA, USPS, and VA. Their comments are reprinted in appendices II through VII, respectively.

Of the six agencies to which we made recommendations, four of them (Commerce, SSA, USPS, and VA) agreed with our recommendations, and one agency (HHS) did not concur with our recommendation. One agency (OMB) did not state whether it agreed or disagreed with our

recommendation. In addition, multiple agencies (GSA, IRS, OMB, USPS, and VA) provided technical comments on the draft report, which we have incorporated, as appropriate.

The following four agencies agreed with the recommendations that we directed to them:

- Commerce agreed with our recommendation. The department stated that it will develop additional guidance to assist federal agencies with alternatives to knowledge-based verification and expects to do so within one year from issuance of this report. Comments from Commerce are reprinted in appendix II.
- SSA agreed with our recommendation. The agency stated that it will continue to seek improvements in its existing remote identity proofing process. SSA also stated that, in addition to a roadmap it developed in fiscal year 2019 to update its knowledge-based verification process to a more secure multi-factor authentication technology, it will take steps to ensure compliance with NIST standards for remote identity proofing. SSA's comments are reprinted in appendix V.
- USPS agreed with our recommendation. The agency stated that it will be developing a roadmap to implement additional identity-proofing tools and techniques through 2020. Comments from USPS are reprinted in appendix VI.
- VA agreed with our recommendation. The department stated that it will develop a specific plan with time frames and milestones to eliminate knowledge-based verification from the aspects of the remote identity proofing process that it controls.

  Further, in its response, VA requested that GAO direct a recommendation to the Department of Defense (DOD) to discontinue DS Logon and consider using Login.gov instead. However, we are not issuing any recommendations to DOD because our scope of work did not include auditing DOD's remote identity proofing processes. Nevertheless, we have adjusted our recommendations to CMS, SSA, USPS, and VA to clarify that Login.gov is one option for identity proofing that they should consider when developing their plans to discontinue the use of knowledge-based verification. VA's comments are reprinted in appendix VII.

One agency did not concur with our recommendation. Specifically, HHS raised several issues related to our findings. The agency stated that it uses a risk-based approach to designing systems controls and that a unilateral prohibition on the use of knowledge-based verification without

alternatives is not a feasible solution. We agree with this comment and strongly support a risk-based approach to designing security controls, as required by FISMA. However, we believe that alternatives to knowledge-based verification exist that should be assessed and incorporated as appropriate. Similarly, HHS noted that for other applications across the department, it has considered factors such as consumer user experience, cost, and operational feasibility in addition to NIST guidelines. We agree that many factors need to be considered in assessing what method or methods of identity proofing are most appropriate for any given application but believe it is important for agencies to develop plans for addressing those factors that also eliminate the use of risky techniques, such as knowledge-based verification, that could have a negative impact on consumers and agencies.

In response to our specific recommendation to CMS, HHS stated that it does not believe that suitable alternative methods exist that would work for CMS' population of users, such as those in the rural community, due to distance or individuals without cell phones. However, we continue to believe that CMS should develop a plan to discontinue the use of knowledge-based verification. We recognize that there are members of the population that may not be reached with certain identity proofing techniques; however, a variety of alternative methods to knowledge-based verification are available that CMS can consider to address the population it serves. Comments from HHS are reprinted in appendix III.

In addition, OMB did not state whether it agreed or disagreed with our recommendation. Further, in an email response, OMB staff from the office of the Federal Chief Information Officer provided a technical comment, which we incorporated. However, OMB did not otherwise comment on the report findings or our recommendation made to the agency.

The IRS also provided written comments on the draft report. In its comments, the agency described the status of its efforts to strengthen identity verification processes, including the fact that it has eliminated the use of knowledge-based verification. Comments from IRS are reprinted in appendix IV. Finally, GSA provided only technical comments on the draft report, as previously mentioned.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to the appropriate congressional committees, to the Administrators of the Centers for Medicare and Medicaid Services and General Services Administration;

the Commissioners of Internal Revenue and Social Security; Director of the Office of Management and Budget; the Postmaster General of the United States; and the Secretaries of the Departments of Commerce and Veterans Affairs. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov, or Michael Clements at (202) 512-8678 or clementsm@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix VIII.

Nick Marinos
Director, Information Technology and Cybersecurity

Michael Clements
Director, Financial Markets and Community Investment

List of Congressional Requesters
The Honorable Ron Wyden
Ranking Member
Committee on Finance
United States Senate
The Honorable Elizabeth Warren
Ranking Member
Subcommittee for Financial Institutions and Consumer Protection
Committee on Banking, Housing, and Urban Affairs
United States Senate
The Honorable Elijah E. Cummings
Chairman
The Honorable Jim Jordan
Ranking Member
Committee on Oversight and Reform
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) describe selected federal agency practices for remote identity proofing of individuals seeking access to major web-based applications using services provided by consumer reporting agencies and the risks associated with those practices, (2) assess selected federal agencies' actions to ensure the effectiveness of agencies' remote identity proofing processes, and (3) assess the sufficiency of federal identity proofing guidance developed by OMB and NIST in assuring the security of federal systems.

To address the first objective, we made an initial, non-probability selection of federal agencies that (1) maintained major public-facing web applications to provide access to federal benefits or services and (2) relied on identity proofing solutions provided by the three nationwide consumer reporting agencies (CRAs)—Equifax, Experian, and TransUnion—to verify the identities of individuals applying for such benefits or services. We considered a "major" application to be one that could involve interaction with millions of individuals across the entire country. To select six agencies from this group, we reviewed prior GAO reports to identify potential agencies for review. We then interviewed officials at these agencies and at CRAs to confirm that these agencies use CRAs as part of their identity proofing processes and to obtain information about additional federal agencies that also employ CRAs for identity proofing for major applications. We included GSA in these interviews because its mission is to support federal agencies and it was likely to be aware of additional federal agencies that fit our criteria. From the information we gained from our interviews and research, we selected these six agencies: the Centers for Medicare and Medicaid Services (CMS), General Services Administration (GSA), Internal Revenue Service (IRS), Social Security Administration (SSA), United States Postal Service (USPS), and the Department of Veterans Affairs (VA).

At each of these agencies, we reviewed documentation that described the current remote identity proofing processes the agencies are using for their major public-facing web applications. In addition, we interviewed agency officials responsible for identity proofing to obtain details of the techniques used to verify remote users of these applications. To the extent that these

entities used CRAs to conduct knowledge-based verification as part of their remote identity-proofing processes, we discussed the risks associated with using knowledge-based methods as well as the potential advantages and limitations of using alternative methods that are not knowledge-based. We also obtained information from officials at NIST about the risks of knowledge-based methods and the availability of alternative methods.

To address the second objective, we assessed remote identity proofing processes used by the selected agencies to determine the extent that they rely on knowledge-based verification to enroll online applicants for federal benefits and services. We also identified alternative methods used by these agencies, either in place of or in addition to knowledge-based verification, and assessed the extent to which agencies had implemented these methods to mitigate the risk of using knowledge-based methods. We compared the remote identity proofing processes at these agencies with the requirements as specified in NIST Special Publication 800-63, *Digital Identity Guidelines*, to determine whether the processes met the requirements of the NIST guidance. We also interviewed officials responsible for these identity proofing programs to obtain information about agencies' plans, if any, to eliminate the use of knowledge-based verification from their remote identity proofing processes in the future and obtained relevant documentation of such plans.

To address the third objective, we reviewed NIST Special Publication 800-63, *Digital Identity Guidelines*, to identify federal requirements for remote identity proofing. We compared the guidance to the *Control Objectives for Information and Related Technologies* (COBIT), a framework of best practices for IT governance, to determine whether the NIST guidance contained clear direction, including relevant and usable guidance, to ensure that those implementing the technology have a clear understanding of what needs to be delivered and how. To assess the sufficiency of this guidance, we consulted with subject matter experts at NIST, ID.me, a private-sector provider of remote verification technologies, and relevant officials at the selected federal entities. Based on information we had obtained about available alternative methods, we determined the extent to which gaps existed in the NIST guidance with regard to implementation of alternative technologies. We also obtained the views of federal agency officials on the extent to which NIST guidance provided sufficient direction to assist them in implementing appropriate remote identity proofing methods.

Further, we reviewed OMB's draft *Identity, Credential, and Access Management* policy and compared it to the requirements in FISMA and identified shortfalls. We also interviewed OMB staff to discuss the sufficiency of the office's current guidance and to determine whether the office planned to issue additional guidance establishing reporting requirements for federal entities or conduct other forms of oversight of federal entities' implementation of the NIST identity proofing guidance.

We conducted this performance audit from November 2017 to May 2019 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the Department of Commerce

UNITED STATES DEPARTMENT OF COMMERCE
The Secretary of Commerce
Washington, D.C. 20230

April 23, 2019

Mr. Nicolas Marinos
Director, Cybersecurity and Data Protection Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Marinos:

Thank you for the opportunity to review and comment on the Government Accountability Office's (GAO) draft report titled *Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes* (GAO-19-288).

On behalf of the Department of Commerce, I have enclosed our comments on the draft report. We concur with the recommendation to the Department of Commerce and will take steps to implement it.

If you have any questions, please contact MaryAnn Mausser, Department of Commerce Audit Liaison, at (202) 482-8120.

Sincerely,

Wilbur Ross

Wilbur Ross

Enclosure

Department of Commerce's Comments on
GAO Draft Report titled
Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes
(GAO-19-288)

The Department of Commerce has reviewed the draft report, and we offer the following comments for GAO's consideration.

Comments on Recommendations
The Government Accountability Office (GAO) made one recommendation to the Department of Commerce in the report.

- **Recommendation**: The Director of the National Institute of Standards and Technology (NIST) should supplement the agency's 2017 technical guidance with additional guidance to assist federal agencies in determining and implementing alternatives to knowledge-based verification that are most suitable for their applications.

  Commerce Response: The Department of Commerce agrees with this recommendation.

  The National Institute of Standards and Technology will develop additional guidance to assist federal agencies with alternatives to knowledge-based verification. We expect to complete this action within one year from issuance of the final GAO report.

Appendix III: Comments from the Department of Health and Human Services

DEPARTMENT OF HEALTH & HUMAN SERVICES

OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

MAY 0 1 2019

Nick Marinos
Director, Cybersecurity and Data Protection Issues
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. Marinos:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, "*Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes*" (GAO-19-288).

The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

Matthew D. Bassett
Assistant Secretary for Legislation

Attachment

GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED –DATA PROTECTION: FEDERAL AGENCIES NEED TO STRENGTHEN ONLINE IDENTITY VERIFICATION PROCESSES (GAO-19-288)

The U.S. Department of Health and Human Services (HHS) appreciates the opportunity to review and comment on the Government Accountability Office's (GAO) draft report on online identity verification processes. HHS takes seriously its role in protecting consumers who utilize HHS systems from identity fraud.

HHS utilizes a risk-based approach to designing system controls related to verification of identity. HHS also considers the system's consumers when designing such controls. Just as knowledge-based verification would not be suitable for the goals of every system, a unilateral prohibition on the use of knowledge-based verification without viable alternatives is not a feasible solution. In addition, federal requirements must be taken into consideration along with customer experience and audience capabilities in evaluating acceptable risks and appropriate processes for identity proofing that also account for usability and accessibility.

To support the implementation of HealthCare.gov, the Centers for Medicare & Medicaid Services (CMS) considered many factors, including National Institute of Standards and Technology (NIST) guidelines, consumer user experience, cost, and operational feasibility in order to develop an automated approach for verifying individuals' identities, called identity proofing, during the user registration and account creation process. Since 2013, CMS has implemented a similar approach for over fifty CMS business applications. This approach verifies identities in adherence to NIST 800-63 guidance for Digital Identity while also considering the need to provide a cost effective and operationally efficient way of confirming the identity of millions of persons creating an account. Improvements to the automated identity proofing process have been implemented over the years to increase the chances of a user getting positively identity proofed while maintaining an appropriate information security risk profile for CMS.

As GAO notes in this report, while NIST has issued guidance to agencies related to identity proofing, it is not sufficient in assisting agencies to adopt secure alternative methods for remote identity proofing. Further, at this time, additional guidance has not been issued to CMS regarding how to implement the NIST guidelines. The alternatives to knowledge-based verification proposed by GAO in their report are not suitable for certain populations served by CMS as they would create undue burden, create barriers to accessing federal services, or may be cost prohibitive. For example, in-person for rural populations is not viable due to travel distance. However, HHS will continue to monitor for potential effective alternatives to knowledge-based verification.

GAO's recommendation and HHS' response is below.

Recommendation
The Administrator of CMS should develop a plan with time frames and milestones to discontinue knowledge-based verification.

HHS Response
HHS does not concur with this recommendation. As mentioned above, existing alternatives to knowledge-based verification, such as mobile device verification and in-person verification, are

GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED –DATA PROTECTION: FEDERAL AGENCIES NEEDTO STRENGTHEN ONLINE IDENTITY VERIFICATION PROCESSES (GAO-19-288)

not suitable for certain populations served by CMS, such as consumers who utilize HealthCare.gov. In the absence of viable alternatives to knowledge-based verification, HHS will continue to monitor for potential effective solutions and, if any become available, utilize them as appropriate and feasible. HHS will look forward to future guidance from NIST and OMB to help guide any changes.

Appendix IV: Comments from the Internal Revenue Service

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

DEPUTY COMMISSIONER

April 29, 2019

Mr. Nick Marinos
Director, Cybersecurity & Data Protection Issues
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Marinos:

Thank you for the opportunity to comment on the draft report titled *Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes* (GAO-19-288). I appreciate the time your staff has taken to speak to representatives of the Internal Revenue Service, Information Technology organization to learn more about how the IRS Secure Assess platform helps protect online tools. As we explained during the audit, the IRS discontinued the use of knowledge-based verification in 2016.

The IRS has made significant progress in strengthening identity protections through the use of Secure Access, which is more secure than any knowledge-based verification process, including verification through mobile device confirmation codes and financial verification via a third party. According to NIST 63-3 guidelines, this approach is considered as fair evidence and provides the IRS additional assurance about an individual's identity.

As GAO states in its report, federal agencies rely on NIST and OMB for guidance and until that guidance is available, a federal agency's ability to unilaterally strengthen identify proofing processes remains challenging. Although certain technologies are not commercially available, we continue working closely with our federal agency partners to find solutions that work, including solutions for those who do not possess cell phones or have internet access. We also continue to invest in multiple layers of defense that secure and protect taxpayer data, with 24/7 monitoring and defense mechanisms embedded throughout IRS systems and online portals.

If you have any questions, please contact me or the IRS Chief Information Officer at (202) 317-5000.

Sincerely,

Jeffrey J. Tribiano

Appendix V: Comments from the Social Security Administration

SOCIAL SECURITY
Office of the Commissioner

April 24, 2019

Mr. Nick Marinos.
Director, Cybersecurity and Data Protection Issues
United States Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Marinos,

Thank you for the opportunity to review the draft report, "DATA PROTECTION: Federal Agencies Need to Strengthen Online Identity Verification Processes" (GAO-19-288). Please see our enclosed comments.

If you have any questions, please contact me at (410) 965-9704. Your staff may contact Trae Sommer, Acting Director of the Audit Liaison Staff, at (410) 965-9102.

Sincerely,

Stephanie Hall

Stephanie Hall
Acting Deputy Chief of Staff

Enclosure

SOCIAL SECURITY ADMINISTRATION BALTIMORE, MD 21235-0001

SSA COMMENTS ON THE GOVERNMENT ACCOUNTABILITY OFFICE (GAO) DRAFT REPORT, "DATA PROTECTION: FEDERAL AGENCIES NEED TO STRENGTHEN ONLINE IDENTITY VERIFICATION PROCESSES" (GAO-19-288)

Safeguarding customer information and proactively mitigating cyber threat is of utmost importance in maintaining the integrity and confidentiality of our digital data. Although today's digital environment presents new and unique challenges, we continue to seek improvements in our existing identity-proofing and authentication processes. In fiscal year 2019, we developed a roadmap to upgrade our knowledge-based verification process to a more secure multi-factor authentication technology. In addition, we are taking steps to ensure compliance with applicable National Institute of Science and Technology standards for digital identity-proofing.

SSA's Recommendation 1 -- GAO's Recommendation 5

The Commissioner of Social Security should develop a plan with specific milestones to discontinue knowledge-based verification.

Response

We agree.

Appendix VI: Comments from the United States Postal Service

UNITED STATES POSTAL SERVICE

April 26, 2019

Mr. Nicholas Marinos
Director, Information Technology
United States Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

SUBJECT: Response to Draft Report: *Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes* (GAO-19-288)

Dear Mr. Marinos:

Thank you for the opportunity to respond to the Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes draft report. Cybersecurity remains a top priority across the Postal Service, and USPS intends to reduce or eliminate the use of knowledge-based verification in the near future with a plan currently being developed to roll out a process that will reduce knowledge-based dependency. As we continue to modernize our information security framework, the focus of the ongoing transformation efforts is to better protect customers, employees, and the enterprise from present-day and future threats.

Management understands the intent of the draft report is to help improve the overall posture and capabilities of strengthening remote identity proofing processes by discontinuing knowledge-based verification. The Postal Service understands the risks associated with the continuous use of knowledge-based verification and has taken many proactive steps to promote a stronger remote identity proofing practice. Management looks forward to working in partnership with the Government Accountability Office to strengthen remote identity proofing leading practices.

475 L'ENFANT PLAZA SW
WASHINGTON DC 20260
WWW.USPS.COM

Recommendation [6]:
The Postmaster General of the United States should develop a plan with time frames and milestones to discontinue knowledge-based verification.

Management Response/Action Plan:
Management agrees with this recommendation. A strategy for discontinuing knowledge-based verification by implementing dynamic identity proofing approaches has been developed and the first phase of that will be implementing a mobile phone verification with a one-time passcode which is in pilot mode today. USPS plans to roll out the mobile phone verification capability to replace the knowledge-based verification by December 2019. USPS will also be creating a roadmap that will map out the implementation of other dynamic identity-proofing tools through 2020.

Gregory S. Crabb
Vice President, Chief Information Security Officer

cc: *Manager, Corporate Audit Response Management*

Appendix VII: Comments from the Department of Veterans Affairs

THE SECRETARY OF VETERANS AFFAIRS
WASHINGTON
APR 2 3 2019

Mr. Michael Clements
Director
Financial Markets and Community Investment
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Clements:

The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office (GAO) draft report: ***DATA PROTECTION: Federal Agencies Need to Strengthen Online Identity Verification Processes*** (GAO-19-288).

The enclosure provides technical comments and sets forth the actions to be taken to address the draft report recommendation.

VA appreciates the opportunity to comment on your draft report.

Sincerely,

Robert L. Wilkie

Enclosure

THE SECRETARY OF VETERANS AFFAIRS
WASHINGTON
APR 23 2019

Mr. Nick Marinos
Director
Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Marinos:

The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office (GAO) draft report: ***DATA PROTECTION: Federal Agencies Need to Strengthen Online Identity Verification Processes*** (GAO-19-288).

The enclosure provides technical comments and sets forth the actions to be taken to address the draft report recommendation.

VA appreciates the opportunity to comment on your draft report.

Sincerely,

Robert L. Wilkie

Enclosure

Enclosure

Department of Veterans Affairs (VA) Comments to
Government Accountability Office (GAO) Draft Report
DATA PROTECTION: Federal Agencies Need to Strengthen Online Identity Verification Processes
(GAO-19-288)

Recommendation 7: The Secretary of the Department of Veterans Affairs should develop a plan with time frames and milestones to discontinue knowledge-based verification.

VA Comment: Concur. VA currently uses two different providers to conduct remote identity proofing of Servicemembers and Veterans applying for VA benefits: Department of Defense (DOD) DS Logon and an identity-proofing contractor, ID.Me.

For eBenefits, the agency uses DS Logon to authenticate users. DS Logon is a DOD-run shared service. Because VA does not control DS Logon, VA is unable to make the necessary changes to the system to discontinue knowledge-based verification. VA and DoD want to continue use of a shared credential, issued prior to discharge. Therefore, VA respectfully requests a recommendation be directed at VA and DoD to discontinue DS Logon, and consider use of GSA's login.gov.

For those credentials that VA does control, VA concurs with GAO's recommendation and will develop a plan with time frames and milestones to discontinue knowledge-based verification. VA will provide more detailed information regarding the plan in our 180-day update to GAO's final report.

1

Appendix VIII: GAO Contacts and Staff Acknowledgments

GAO Contacts

Nick Marinos, (202) 512-9342, MarinosN@gao.gov

Michael Clements, (202) 512-8678, ClementsM@gao.gov

Staff Acknowledgments

In addition to the individuals named above, John de Ferrari and John Forrester (assistant directors); Tina Torabi (analyst-in-charge); Bethany Benitez, Christina Bixby, Chris Businsky, Kavita Daitnarayan, Nancy Glover, Andrea Harvey, Thomas Johnson, David Plocher, Rachel Siegel, and Winnie Tsen made key contributions to this report.

Appendix IX: Accessible Data

Agency Comment Letters

Accessible Text for Appendix II Comments from the Department of Commerce

Page 1

April 23, 2019

Mr. Nicolas Marinos

Director, Cybersecurity and Data Protection Issues

U.S. Government Accountability Office

441 G Street, NW

Washington, DC 20548

Dear Mr. Marinos:

Thank you for the opportunity to review and comment on the Government Accountability Office's (GAO) draft report titled Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes (GAO-19-288).

On behalf of the Department of Commerce, I have enclosed our comments on the draft report. We concur with the recommendation to the Department of Commerce and will take steps to implement it.

If you have any questions, please contact MaryAnn Mausser, Department of Commerce Audit Liaison, at (202) 482-8120.

Sincerely,

Wilbur Ross

Enclosure

Page 2

Department of Commerce's Comments on GAO Draft Report titled

Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes

(GA0-19-288)

The Department of Commerce has reviewed the draft report, and we offer the following comments for GAO's consideration.

Comments on Recommendations

The Government Accountability Office (GAO) made one .recommendation to the Department of Commerce in the report.

- Recommendation: The Director of the National Institute of Standards and Technology (NIST) should supplement the agency's 2017 technical guidance with additional guidance to assist federal agencies in determining and implementing alternatives to knowledge-based verification that are most suitable for their applications.

Commerce Response: The Department of Commerce agrees with this recommendation.

The National Institute of Standards and Technology will develop additional guidance to assist federal agencies with alternatives to knowledge-based verification. We expect to complete this action within one year from issuance of the final GAO report.

Accessible Text for Appendix III Comments from the Department of Health and Human Services

Page 1

MAY 01 2019

Nick Marinos

Director, Cybersecurity and Data Protection Issues

U.S. Government Accountability Office

441 G Street NW

Washington, DC 20548

Dear Mr. Marinos:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, "Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes" (GAO-19-288).

The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

Matthew D. Bassett

Assistant Secretary for Legislation

Attachment

Page 2

The U.S. Department of Health and Human Services (HHS) appreciates the opportunity to review and comment on the Government Accountability Office's (GAO) draft report on online identity verification processes. HHS takes seriously its role in protecting consumers who utilize HHS systems from identity fraud.

HHS utilizes a risk-based approach to designing system controls related to verification of identity. HHS also considers the system's consumers when designing such controls. Just as knowledge-based verification would not be suitable for the goals of every system, a unilateral prohibition on the use of knowledge-based verification without viable alternatives is not a feasible solution. In addition, federal requirements must be taken into consideration along with customer experience and audience capabilities in evaluating acceptable risks and appropriate processes for identity proofing that also account for usability and accessibility.

To support the implementation of HealthCare.gov, the Centers for Medicare & Medicaid Services (CMS) considered many factors, including National Institute of Standards and Technology (NIST) guidelines, consumer user experience, cost, and operational feasibility in order to develop an automated approach for verifying individuals' identities , called identity proofing, during the user registration and account creation process. Since 2013, CMS has implemented a similar approach for over fifty CMS business applications. This approach verifies identities in adherence to NIST 800-63 guidance for Digital Identity while also considering the need to provide a cost effective and operationally efficient way of confirming the identity of millions of persons creating an account. Improvements to the automated identity proofing process have been implemented over the years to increase the chances of a user getting positively identity proofed while maintaining an appropriate information security risk profile for CMS.

As GAO notes in this report, while NIST has issued guidance to agencies related to identity proofing, it is not sufficient in assisting agencies to adopt secure alternative methods for remote identity proofing. Further, at this time, additional guidance has not been issued to CMS regarding how to implement the NIST guidelines. The alternatives to knowledge-based verification proposed by GAO in their report are not suitable for certain populations served by CMS as they would create undue burden, create barriers to accessing federal services, or may be cost prohibitive. For example in-person for rural populations is not viable due to travel distance. However, HHS will continue to monitor for potential effective alternatives to knowledge-based verification.

GAO's recommendation and HHS' response is below.

Recommendation

The Administrator of CMS should develop a plan with time frames and milestones to discontinue knowledge-based verification.

HHS Response

HHS does not concur with this recommendation. As mentioned above, existing alternatives to knowledge-based verification, such as mobile device verification and in-person verification, are

Page 3

not suitable for certain populations served by CMS, such as consumers who utilize HealthCare.gov. In the absence of viable alternatives to knowledge-based verification, HHS will continue to monitor for potential effective solutions and, if any become available, utilize them as appropriate and feasible. HHS will look forward to future guidance from NIST and 0MB to help guide any changes.

Accessible Text for Appendix IV Comments from the Internal Revenue Service

April 29, 2019

Mr. Nick Marinos

Director, Cybersecurity & Data Protection Issues

U.S. Government Accountability Office

441 G Street, N.W.

Washington, D.C. 20548

Dear Mr. Marinos:

Thank you for the opportunity to comment on the draft report titled Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes (GAO-19-288). I appreciate the time your staff has taken to speak to representatives of the Internal Revenue Service, Information Technology organization to learn more about how the IRS Secure Assess platform helps protect online tools. As we explained during the audit, the IRS discontinued the use of knowledge-based verification in 2016.

The IRS has made significant progress in strengthening identity protections through the use of Secure Access, which is more secure than any knowledge-based verification process, including verification through mobile device confirmation codes and financial verification via a third party. According to NIST 63-3 guidelines, this approach is considered as fair evidence and provides the IRS additional assurance about an individual's identity.

As GAO states in its report, federal agencies rely on NIST and 0MB for guidance and until that guidance is available, a federal agency's ability to unilaterally strengthen identify proofing processes remains challenging. Although certain technologies are not commercially available, we continue working closely with our federal agency partners to find solutions that work, including solutions for those who do not possess cell phones or have internet access. We also continue to invest in multiple layers of defense that secure and protect taxpayer data, with 24/7 monitoring and defense mechanisms embedded throughout IRS systems and online portals.

If you have any questions, please contact me or the IRS Chief Information Officer at (202) 317-5000.

Sincerely,

Jeffrey J. Tribiano

Accessible Text for Appendix V Comments from the Social Security Administration

Page 1

April 24, 2019

Mr. Nick Marinos.

Director, Cybersecurity and Data Protection Issues

United States Government Accountability Office

441 G Street, NW

Washington, DC 20548

Dear Mr. Marinos,

Thank you for the opportunity to review the draft report, “DATA PROTECTION: Federal Agencies Need to Strengthen Online Identity Verification Processes” (GAO-19-288). Please see our enclosed comments.

If you have any questions, please contact me at (410) 965-9704. Your staff may contact Trae Sommer, Acting Director of the Audit Liaison Staff, at (410) 965-9102.

Sincerely,

Stephanie Hall

Acting Deputy Chief of Staff

Enclosure

Page 2

Safeguarding customer information and proactively mitigating cyber threat is of utmost importance in maintaining the integrity and confidentiality of our digital data. Although today's digital environment presents new and unique challenges, we continue to seek improvements in our existing identity- proofing and authentication processes. In fiscal year 2019, we developed a roadmap to upgrade our knowledge-based verification process to a more secure multi-factor authentication technology. In addition, we are taking steps to ensure compliance with applicable National Institute of Science and Technology standards for digital identity-proofing.

SSA's Recommendation 1 -- GAO's Recommendation 5

The Commissioner of Social Security should develop a plan with specific milestones to discontinue knowledge-based verification.

Response

We agree.

Accessible Text for Appendix VI Comments from the United States Postal Service

Page 1

April 26, 2019

Mr. Nichoias Marinos

Director, Information Technology

United States Government Accountability Office

441 G Street, NW

Washington, DC 20548-0001

SUBJECT: Response to Draft Report: Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes (GAO-19-288)

Dear Mr. Marinos:

Thank you for the opportunity to respond to the Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes draft report. Cybersecurity remains a top priority across the Postal Service, and USPS intends to reduce or eliminate the use of knowledge-based verification in the near future with a plan currently being developed to roll out a process that will reduce knowledge-based dependency. As we continue to modernize our information security framework, the focus of the ongoing transformation efforts is to better protect customers, employees, and the enterprise from present-day and future threats.

Management understands the intent of the draft report is to help improve the overall posture and capabilities of strengthening remote identity proofing processes by discontinuing knowledge-based verification. The Postal Service understands the risks associated with the continuous use of knowledge-based verification and has taken many proactive steps to promote a stronger remote identity proofing practice. Management looks forward to working in partnership with the Government Accountability Office to strengthen remote identity proofing leading practices.

Page 2

Recommendation [6]:

The Postmaster General of the United States should develop a plan with time frames and milestones to discontinue knowledge-based verification.

Management Response/Action Plan:

Management agrees with this recommendation. A strategy for discontinuing knowledge-based verification by implementing dynamic

identity proofing approaches has been developed and the first phase of that will be implementing a mobile phone verification with a one-time passcode which is in pilot mode today. USPS plans to roll out the mobile phone verification capability to replace the knowledge-based verification by December 2019. USPS will also be creating a roadmap that will map out the implementation of other dynamic identity-proofing tools through 2020.

Gregory S. Crabb

Vice President, Chief Information Security Officer

cc: Manager, Corporate Audit Response Management

Accessible Text for Appendix VII Comments from the Department of Veterans Affairs

Page 1

APR 23 2019

Mr. Michael Clements

Director

Financial Markets and Community Investment

U.S. Government Accountability Office

441 G Street, NW

Washington, DC 20548

Dear Mr. Clements:

The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office (GAO) draft report: DATA PROTECTION: Federal Agencies Need to Strengthen Online Identity Verification Processes (GAO-19-288).

The enclosure provides technical comments and sets forth the actions to be taken to address the draft report recommendation.

VA appreciates the opportunity to comment on your draft report.

Sincerely,

Robert L. Wilkie

Enclosure

Page 2

APR 23 2019

Mr. Nick Marinos Director

Information Technology and Cybersecurity

U.S. Government Accountability Office

441 G Street, NW

Washington, DC 20548

Dear Mr. Marinos:

The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office (GAO) draft report: DATA PROTECTION: Federal Agencies Need to Strengthen Online Identity Verification Processes (GAO-19-288).

The enclosure provides technical comments and sets forth the actions to be taken to address the draft report recommendation.

VA appreciates the opportunity to comment on your draft report.

Sincerely,

Robert L. Wilkie

Enclosure

Page 3

Recommendation 7: The Secretary of the Department of Veterans Affairs should develop a plan with time frames and milestones to discontinue knowledge-based verification.

VA Comment: Concur. VA currently uses two different providers to conduct remote identity proofing of Servicemembers and Veterans applying for VA benefits: Department of Defense (DOD) OS Logon and an identity-proofing contractor, ID.Me.

For eBenefits, the agency uses OS Logon to authenticate users. OS Logan is a DOD- run shared service. Because VA does not control OS Logan, VA is unable to make the necessary changes to the system to discontinue knowledge-based verification. VA and DoD want to continue use of a shared credential, issued prior to discharge. Therefore, VA respectfully requests a recommendation be directed at VA and DoD to discontinue OS Logon, and consider use of GSA's login.gov.

For those credentials that VA does control, VA concurs with GAO's recommendation and will develop a plan with time frames and milestones to discontinue knowledge- based verification. VA will provide more detailed information regarding the plan in our 180-day update to GAO's final report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (https://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to https://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/fraudnet/fraudnet.htm

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548