GAO Highlights

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

May 2019

DATA PROTECTION

Federal Agencies Need to Strengthen Online Identity Verification Processes

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.