Office of Inspections
Office of Inspector General
U.S. General Services Administration

GSA Misled Customers on Login.gov's Compliance with Digital Identity Standards

JE23-003 (Redacted)
March 7, 2023

Introduction

In April 2022, the Office of Inspector General (OIG), Office of Inspections, initiated an evaluation of the U.S. General Services Administration's (GSA) Login.gov services. We initiated this evaluation based on a notification received from GSA's Office of General Counsel identifying potential misconduct within Login.gov, a component of GSA's Technology Transformation Services (TTS) under the Federal Acquisition Service (FAS).

Our evaluation found GSA misled their customer agencies when GSA failed to communicate Login.gov's known noncompliance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3, *Digital Identity Guidelines*.[1] Notwithstanding GSA officials' assertions that Login.gov met SP 800-63-3 Identity Assurance Level 2 (IAL2) requirements, Login.gov has never included a physical or biometric comparison for its customer agencies. Further, GSA continued to mislead customer agencies even after GSA suspended efforts to meet SP 800-63-3.

GSA knowingly billed IAL2 customer agencies over $10 million for services, including alleged IAL2 services that did not meet IAL2 standards. Furthermore, GSA used misleading language to secure additional funds for Login.gov. Finally, GSA lacked adequate controls over the Login.gov program and allowed it to operate under a hands-off culture. We found that because of its failure to exercise management oversight and internal controls over Login.gov, FAS shares responsibility for the misrepresentations to GSA's customers. We make five recommendations to address the findings in this report. In response to our report, GSA management agreed with our findings and recommendations. Management comments can be found in their entirety in Appendix 2.

Background

Federal cybersecurity requirements obligate the Administrator of the General Services Administration, in collaboration with the Secretary of Homeland Security, to develop a single sign-on trusted identity platform that the head of each agency, with exceptions, shall implement for individuals accessing each public website of the agency that requires user authentication.[2]

[1] NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems.

[2] 6 U.S.C. 1523(b)(1)(D) (Pub. L. 114–113, div. N, title II, §225, Dec. 18, 2015, 129 Stat. 2967).

In 2016, the GSA Technology Transformation Service 18F division initiated a project to build a multi-factor authentication login platform that would generate a single account for users interacting with the federal government online.[3] GSA describes 18F as a "technology and design consultancy for the U.S. Government inside the government" which "partners with agencies to improve the user experience of government services by helping them build and buy technology."[4] The intent for the login platform was "to create a seamless, secure, and user-friendly 'lock' to the government's digital services."[5] In April 2017, GSA launched Login.gov as "a single sign-on solution for government websites that will enable citizens to access public services across agencies with the same username and password."[6]

In June 2017, NIST issued Special Publication 800-63-3*, Digital Identity Guidelines* (SP 800-63-3), along with Special Publication 800-63A, *Digital Identity Guidelines, Enrollment and Identity Proofing* (SP-800-63A), and Special Publication 800-63-3B, *Digital Identity Guidelines, Authentication and Lifecycle Management* (SP-800-63B). The SP 800-63 suite of publications, which currently includes updates through March 2, 2020, sets the baseline requirements for digital identity services, and addresses risks associated with authentication and identify proofing errors.[7]

SP 800-63-3 provides technical requirements and guidance for identity proofing and authentication of users interacting with government information technology systems, such as Login.gov, over open networks.[8] NIST distinguishes between "normative" material that is "mandatory" and "informative" material that provides guidance but does not present mandatory requirements.[9]

---

[3] 18F initially was part of FAS and became part of a new service-level component, Technology Transformation Service, created in 2016. The following year, GSA restructured the new service as a similarly named component within FAS, Technology Transformation Services, that included 18F.

[4] https://18f.gsa.gov.

[5] https://18f.gsa.gov/2016/05/10/building-a-modern-shared-authentication-platform/.

[6] https://18f.gsa.gov/2017/08/22/government-launches-login-gov/.

[7] SP-800-63-3, at pgs. 22, 23 (pdf. 34-35/75). The NIST "suite of publications" also includes SP 800-63-3C, *Digital Identity Guidelines, Federation and Assertions*, but it is not relevant to this report.

[8] SP 800-63-3, at pg. iii.

[9] SP 800-63-3, at pg. v. Mandatory verbs are "SHALL," "SHALL NOT," and "CANNOT". The informative terms are "SHOULD NOT," "MAY," "NEED NOT," and "CAN." NIST provides specific definitions for each term that apply when a NIST identify proofing and authentication publication capitalizes words. *Id*.; NIST SP-800-63B at iii (Requirements Notation and Conventions).

According to NIST:

> Identity proofing establishes that a subject is who they claim to be. Digital authentication establishes that a subject attempting to access a digital service is in control of one or more valid authenticators associated with that subject's digital identity.[10]

The Office of Management and Budget, subsequently in May 2019, issued Memorandum M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*, requiring federal agencies to implement SP 800-63-3 and any successive versions.[11] Additionally, Memorandum M-19-17 required agencies to use federally provided or commercially provided shared services, to the extent available, to deliver identity assurance and authentication services to the public. Implementation of SP 800-63-3 required a shift from Login.gov's multi-factor authentication platform to a two-component risk-based process – Identity Assurance Level (IAL) (identity proofing) and Authenticator Assurance Level (AAL) (authentication).

The NIST framework for both IAL and AAL provides three levels of risk mitigation that agencies may select. For IAL, an agency chooses an option based on their risk profile and the *potential harm from an attacker falsely claiming an identity*. For AAL, an agency chooses an option based on their risk profile and the potential harm of an attacker *taking control of an authenticator and accessing the agency's systems*.[12]

SP 800-63A details the requirements for identity proofing at each IAL including the physical presence of the applicant, evidence collection, validation, and verification. At IAL2 identity proofing, the presence requirement may be accomplished remotely or in-person. NIST categorizes possible evidence to establish identity as "superior," "strong," "fair," and "weak." To meet the IAL2 evidence requirement, collection must include at least one piece of "superior" or "strong," or a combination of "strong" and "fair" evidence.[13]

For identity verification, the goal is to confirm and establish a linkage between the claimed identity and the real-life existence of the subject presenting the evidence.[14] Importantly, identity verification at the "strong" level requires either a physical comparison to a photograph on the

---

[10] *Id. at pg. iv.*

[11] https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf

[12] SP 800-63-3, at pg. vi.

[13] NIST Special Publication 800-63A, *Digital Identity Guidelines, Enrollment and Identity Proofing*, June 2017.

[14] *Id.* at 5.3

strongest piece of evidence provided, or a biometric comparison to the strongest piece of evidence provided. A biometric comparison measures both physical characteristics, such as a facial image (also referred to as a selfie), iris recognition, or fingerprints, and behavioral characteristics, such as typing cadence.[15]

However, when identity verification is performed *remotely* and does not include a remote physical comparison, as in the case of Login.gov, the identity confirmation *must* also include a biometric comparison.[16] Therefore, in order to achieve IAL2 in the Login.gov environment, there must always be a biometric comparison.

In July 2019, the GSA Chief Information Officer (CIO) stated in the Login.gov FedRAMP Agency Authorization to Operate that the system "can support user validation at Identity Assurance Level 1 or 2 (IAL1 or IAL2)." In November 2019, the CIO permitted Login.gov customer deployment of IAL2 services, with certain conditions, including strict limitations on users' personally identifiable information and limiting IAL2 integrations to 2.1 million users in fiscal year 2020, among others. Our evaluation found that despite assertions made by Login.gov officials that they met SP 800-63-3, Login.gov has never included either a physical comparison or biometric comparison available to customer agencies, as required for identity verification at the IAL2 level.[17] Rather than conducting physical or biometric comparisons, Login.gov was instead using a third party to compare identification cards to information contained in LexisNexis®.

Login.gov also dismissed additional safeguards when NIST strengthened the standards for identity verification. Updated in March 2020, SP 800-63B focuses on digital authentication of users interacting with government systems over open networks and recommends that the biometric system *"SHOULD"* implement liveness detection – the technology known as presentation attack detection or PAD.[18] PAD is used to confirm that biometric proof of identity,

---

[15] *Id*. at 5.3.1. See also, NIST Special Publication 800-63B, *Digital Identity Guidelines, Authentication and Lifecycle Management*, at pg. 26: "Biometric characteristics do not constitute secrets. They can be obtained online or by taking a picture of someone with a camera phone (e.g., facial images) with or without their knowledge, lifted from objects someone touches (e.g., latent fingerprints), or captured with high resolution images (e.g., iris patterns)."

[16] *Id*. at Table 5-3, Verifying Identity Evidence, Strong. "For remote physical comparison, the applicants' facial image may be captured by a high resolution video or camera for physical comparison to the facial image photograph on the identity evidence." SP 800-63A Conformance Criteria, pgs. 34-35.

[17] *Id*.

[18] According to SP 800-63-3, pg. v, "SHOULD refers to a technique, technology, or process that is recommended but not mandatory." When capitalized, "SHOULD" is used as one of the verbs "that are internationally recognized in standards organizations as normative and requirements-based." *Id*. When NIST uses the lowercase of "SHALL" and "SHALL NOT," "SHOULD" and "SHOULD NOT," "MAY" and "NEED NOT," and "CAN" and "CANNOT" in the SP 800-63-3 suite of publications and related guidance, the meanings do not apply. For example, "SHALL" is mandatory, but "shall" in NIST publications is not mandatory.

such as a photograph, reflects the live capture of an applicant's selfie. SP 800-63B also notes that liveness detection is being considered as a *mandatory* requirement in future editions.

Just a few months later, NIST released additional guidance for the implementation of SP 800-63-3. The new conformance criteria for SP 800-63A and SP 800-63B, released in June 2020, provided supplemental guidance to clarify requirements and information agencies need in order to meet conformance criterion for purposes of implementation and assessment, including for IAL2.[19] In this guidance, NIST clarified the importance of liveness detection for identity proofing verification of evidence at IAL2.

> Remote identity proofing *requires* the collection of *both* an image of the identity evidence and a live capture of the facial image of the applicant for physical or biometric comparison. The CSP [credential service provider] *must* employ liveness and presentation attack detection capabilities to ensure that the applicant's facial image or other biometric characteristic used for comparison is "live" and not a spoofing or presentation attack.[20] (Emphasis added.)

Subsequently in July 2020, NIST released implementation guidance that reiterated the importance of liveness detection for IAL2 remote identity proofing and added:

> It is noted that liveness detection is a *necessary* control whether the identity verification is performed through physical comparison of the live capture of the applicants' facial image to the photograph on the strongest piece of identity evidence or through automated biometric facial image comparison.[21] (Emphasis added.)

According to the TTS Operations Division, as of May 2022, Login.gov had 906,187 users of Login.gov services that GSA purported to be IAL2 but did not comply with SP 800-63-3 biometric comparison requirements. With regard to liveness detection, GSA also did not follow SP 800-63B's implementation recommendation, and did not employ the NIST June and July 2020 supplemental guidance.

---

[19] *Conformance Criteria* for *NIST SP 800-63A Enrollment and Identity Proofing and NIST SP 800-63B Authentication and Lifecycle Management*, June 2020, pg. 1.

[20] *Conformance Criteria* for *NIST SP 800-63A Enrollment and Identity Proofing and NIST SP 800-63B Authentication and Lifecycle Management*, June 2020, pg. 35.

[21] *NIST Special Publication 800-63-3 Implementation Resources*, July 1, 2020, pgs. 17, 28.

This report focuses on GSA's communications with customer agencies and the public regarding claims that Login.gov met the IAL2 standards.

Findings

Finding 1. Login.gov did not meet NIST requirements for a biometric comparison or employ other protections that NIST recommends.

Notwithstanding GSA officials' assertions that Login.gov met SP 800-63-3 requirements, Login.gov has never included a physical or biometric comparison in production. Login.gov officials informed us that biometric comparison was not included in products offered to customer agencies, initially because the feature required testing before implementation and later because they further delayed it due to equity concerns.[22] Because the version of Login.gov available for customer agency use has never included physical or biometric comparison, it has never met SP 800-63-3 requirements for IAL2. Additionally, Login.gov did not employ other protections that NIST recommends for remote identity proofing.

Login.gov failed to meet NIST IAL2 biometric comparison requirements.

As early as September 2018, Login.gov officials began discussions internally and with potential customer agencies regarding the launch of IAL2 identity proofing services. Login.gov interagency agreements began to include statements such as:

> The login.gov IAL1 service meets NIST 800-63-3 for AAL2 and IAL1.
>
> The login.gov IAL2 service meets NIST 800-63-3 for AAL2 and IAL2.
>
> TTS will provide IAL1 and IAL2 services on a reimbursable basis.

Despite GSA's failure to meet the IAL2 requirements, 18 of Login.gov's 22 interagency agreements executed from September 18, 2018 to July 7, 2021 stated that they included IAL2 services that *met* and/or were *consistent* with the IAL2 requirements.

At the time of the events covered by this report, the Login.gov program had multiple layers of oversight. Immediate managerial supervision came from the Login.gov Director position, and

[22] Executive Order 13985, *Executive Order on Advancing Racial Equity and Support for Underserved Communities Through the Federal Government,* Sec. 2, states that the term "equity" means the consistent and systematic fair, just, and impartial treatment of all individuals. For Login.gov, the equity concerns pertain to physical traits, such as skin color and tone, that may be discriminated against in the identify verification process.

additional oversight went through the TTS Office of Solutions, created in 2019, through the TTS Director/FAS Deputy Commissioner, up to the level of the FAS Commissioner:

- Acting Login.gov Director [redacted] * supervised the program beginning August 2019, when he took over the position from [redacted]. In February 2022, [redacted] stepped in as Acting Login.gov Director. [23]

- In September 2019, Assistant Commissioner Dominic Sale headed the TTS Office of Solutions. In January 2021, [redacted] replaced Sale.

- Vladlen "Dave" Zvenyach became the TTS Director/FAS Deputy Commissioner in January 2021. GSA CIO David Shive and, before him, Bob DeLuca, had been acting in the position after Anil Cheriyan left in July 2020.

- FAS Commissioner Sonny Hashmi oversaw Zvenyach.

At multiple points over the past three years, senior leaders in TTS and Login.gov learned that Login.gov did not comply with IAL2 requirements. They did not, however, notify customer agencies of the noncompliance. The inability to meet IAL2 NIST standards became the topic of discussions among Login.gov leaders and personnel at least as early as 2019, and included concerns that using individuals' selfies to verify their identity could impact Login.gov's rejection rates based on physical traits, such as skin color and tone. Login.gov had intended to use selfies to meet IAL2 standards, and had included the feature in marketing materials as early as 2019. Discussions centering on the selfie concerns continued after TTS Director Zvenyach arrived in 2021, and he participated in those discussions.

A former Login.gov Product Manager, [redacted], told us that the team knew that Login.gov did not comply with NIST 800-63-3 as early as 2018. [redacted] stated that the initial decision to promote Login.gov as meeting SP 800-63-3 for IAL2 was made by [redacted]'s predecessor, Acting Login.gov Director [redacted].

A TTS Senior Advisor (hereafter the Senior Advisor) told us that in January 2020, he alerted [redacted], [redacted], and Assistant Commissioner Sale that Login.gov lacked the biometric comparison necessary for SP 800-63-3 compliance. The Senior Advisor told us that he realized that Login.gov did not meet IAL2 standards and discussed with Sale his concerns about IAL2, as

[23] In February 2022, Zvenyach moved [redacted] to another position within TTS. On September 12, 2022, GSA appointed [redacted] as the Login.gov Director.

*Certain names have been redacted in this report to protect the privacy interests of employees at the grade GS-15 or lower.

well as concerns that customer agencies were not feeling heard and not participating in the product development process. The Senior Advisor stated that Sale told him that because he was not the Director of Login.gov, it was not the Senior Advisor's role to pursue the issue and that he could only advise the program by providing strategy and input to the Login.gov team. The Senior Advisor stated at that point he did not pursue the issue further and he did not escalate his concerns to the TTS Director.[24]

On August 10, 2020, a consultant advising GSA (hereafter the GSA consultant) informed the Senior Advisor and [redacted] that they needed to provide a biometric comparison to be compliant with NIST. The GSA consultant sent [redacted] and the Senior Advisor an email stating that there was "no real way around a biometric for IAL2." [redacted] told us that the email from the consultant signaled to him that Login.gov did not comply with SP 800-63-3 and that he "should have but did not" escalate the noncompliance. [redacted] told us that he believed that everyone knew that Login.gov was not compliant with SP 800-63-3 IAL2 requirements; however, [redacted] again stated that he did not escalate his concerns further.

Rather, [redacted] told us that his focus was on fulfilling partner needs, and not on the SP 800-63-3 standard's requirements. We found a Slack discussion where [redacted] stated, "our product should be chasing after our partner (and users') needs, not after a spec. if the partner *asks* for spec conformance, we should ask why so we get to the *need*." Put simply, Login.gov opted to ignore the standards and instead focused on selling Login.gov to customers without regard to NIST requirements.

We asked [redacted] why GSA did not inform customer agencies of the failure to meet the IAL2 standard. He told us that, in his view, the Login.gov team did meet IAL2 requirements because they were only non-compliant in one area, the biometric comparison – which he considered to be a "flavor" or "spirit" of IAL2. [redacted] acknowledged that the Login.gov team should have updated their interagency agreements to note that Login.gov did not meet SP 800-63-3's biometric requirement. However, he believed that, as a government provider of a national identity verification platform, GSA has "flexibilities" in meeting the SP 800-63-3 requirements. However, SP 800-63-3 states that when requirements are not met, agencies:

> SHALL demonstrate comparability of any chosen alternative, to include any compensating controls when the complete set of applicable SP 800-63 requirements is not implemented.

And

> SHALL implement procedures to document both the justification for any departure from normative requirements and detail the compensating control(s) employed.

[24] Anil Cheriyan served as the FAS Deputy Commissioner/TTS Director from January 2019 to July 2020.

In the case of Login.gov's missing the biometric requirement, GSA had no comparable alternative, no compensating controls, and no documented justification.[25] Login.gov does not provide IAL2 services to customer agencies when those services do not meet the basic requirements of SP 800-63-3, as laid out by NIST. Meeting the "spirit" or "flavor" is not meeting the standard in NIST.

SP 800-63-3 states that it "provide[s] technical requirements for federal agencies implementing digital identity services." As to [redacted]'s claim that GSA has flexibilities in meeting the NIST standard, any such claim lost viability in May 2019 when the Office of Management and Budget issued Memorandum M-19-17, directing in mandatory terms that federal agencies "must implement" SP 800-63-3, including the IAL standards, "in combination with the remaining suite of publications that *relate to* identity management issued by NIST, the Office of Personnel Management (OPM), and the Department of Homeland Security (DHS) to form a comprehensive approach to identity proofing that safeguards privacy and security."[26]

We found that Zvenyach learned about IAL2 problems at least as early as April 13, 2021, when [redacted] and another Login.gov employee briefed Zvenyach on a recent meeting with a customer agency's need for using liveness detection. Zvenyach acknowledged in the same Slack discussion with his team that he was aware that there was a problem with Login.gov's IAL2 services, specifically, "we already know that we're going to struggle with proofing" for some populations. He recognized that "liveness (because it discriminates) can give a false sense of success" and wanted to "look at other, more equitable, proofing options?[sic]." Zvenyach told us, however, that he did not associate the equity of liveness and facial recognition with IAL2 compliance.

Hashmi informed us that in early 2021, Zvenyach told him clearly that Login.gov met the IAL2 standards, and they were signing interagency agreements that stated they met the standard. Nonetheless, Zvenyach told us that he made the ultimate decision not to implement selfie or liveness checks in June 2021. At this point, Zvenyach knew full well that GSA was not moving forward with the selfie-check feature, the biometric comparison that uses a facial image.

According to Zvenyach, he did not discuss IAL2 standards with the Login.gov team until January 2022, when a customer agency asked how Login.gov could meet IAL2 if they did not have facial recognition or biometrics. At that point, Zvenyach said, he determined that Login.gov did not meet the IAL2 standard because they lacked a selfie check.

---

[25] *NIST Special Publication 800-63-3 Digital Identity Guidelines*, at 5.4, Risk Acceptance and Compensating Controls, pg. 22.

[26] M-19-17 at II.

After this, the Senior Advisor told us [redacted] and [redacted] approached him to inquire about compensating controls to achieve IAL2, but he told them he did not see any compensating controls to get around the IAL2 biometric standards. [redacted] told us that Login.gov has since moved away from using terminology like "compensating controls" to instead say they are comparable or equivalent to IAL2. He explained that stating Login.gov has compensating controls for IAL2 implied that Login.gov would be meeting SP 800-63-3, when instead Login.gov's path to comparability is through implementing fraud detection and prevention controls, not selfie and liveness checks, which would allow them to meet a "risk based threshold" for IAL2 comparability.

[redacted] stated in a January 31, 2022 Slack message:

> [O]ur position is that the verification of evidence against a selfie, without liveness, is nowhere near worth the tradeoff in its impact to equity.
>
> We are always considering impacts on usability and accessibility against what the specification says, word for word. In this case, there is a fundamental flaw in suggesting that a selfie check is going to curtail fraud or increase confidence in the proofed identity, without a liveness check.
>
> Our position is that selfie matching is not nearly valuable enough. Only selfie+liveness is valuable in this context. And: liveness/PAD is not a requirement of the spec.

However, the next day, the Senior Advisor told [redacted] in a Slack message, "[I] don't think we have a 'security compensating control' argument," and "yes, we do not comply with NIST IAL2." In response, [redacted] stated, "yyyyeahhhhhhhh we're going to be eating some :crow: [sic]."

GSA finally notified customer agencies on February 3, 2022, that its services were not compliant with SP 800-63-3 (discussed further in Finding 2).

Login.gov also did not employ NIST recommendations for liveness detection.

Originally issued in June 2017, the SP 800-63 suite of publications includes updates through March 2, 2020, including SP 800-63B, which notes that liveness detection SHOULD be implemented, and is being considered as a mandatory requirement in the future. Additional NIST publications related to identity management include the June 2020 conformance criteria and the July 2020 implementation resources. As mentioned above, NIST encouraged IAL2 verification methods in the guidance outlined in the 2020 conformance criteria and implementation resources:

> Remote identity proofing *requires* the collection of both an image of the identity evidence and a live capture of the facial image of the applicant for physical or biometric comparison. *The CSP [Credential Service Provider] must employ liveness detection capabilities* to ensure that the applicant's facial image used for comparison is "live" and not a spoofing or presentation attack.[27] (Emphasis added.)

Based on NIST 2020 conformance criteria and implementation resources, the prudent way to make sure the biometric comparison for IAL2 is more secure is to include liveness detection. We interviewed a NIST senior advisor who explained that while NIST does not use "must" for normative guidance, they used the term "must" for liveness detection to emphasize that even though it is a recommendation, it is an important consideration. The advisor also said that liveness detection, though not required, should be in place to offer a higher level of assurance.

While the conformance criteria and implementation resources do not stipulate compulsory requirements, they do convey that including liveness detection offers a higher level of security and assurance. Nonetheless, GSA did not employ NIST's guidance. Notably, the GSA consultant told us that just using a biometric would *not* be secure, and therefore leave the identity proofing process open to attack without a check for liveness. The consultant stated that fraud detection provided by facial recognition alone is limited.

[redacted] expressed in an April 2021 Slack discussion that "current NIST guidance requires a form of presentation attack defense (PAD) for increased security." He was also included in a Slack discussion with [redacted] in August 2020 in which [redacted] confirmed his understanding that "[Login.gov's] IAL2 solution in production is not NIST conformant because we don't meet the verification requirement (that asks for a liveness test)."[28]

In a Slack discussion on March 2, 2022, [redacted] indicated that he had just become aware of the 2020 NIST guidance on liveness detection:

> huh. has anybody ever seen this before? July 2020 with some very different language around liveness than the spec "The CSP must employ liveness detection capabilities to ensure that the applicant's facial image used for comparison is "live" and not a spoofng [sic] or presentation attack."

---

[27] *NIST Special Publication 800-63-3 Implementation Resources*, July 1, 2020, pgs. 16, 28, and *Conformance Criteria* for *NIST SP 800-63A Enrollment and Identity Proofing and NIST SP 800-63B Authentication and Lifecycle Management*, June 2020, pg. 35.

[28] As noted earlier, although both [redacted] and [redacted] concluded that NIST required liveness, neither the June 2020 nor the July 2020 guidance was mandatory.

Although [redacted] and [redacted] were aware of the supplemental guidance on liveness and PAD as early as August 2020, they did not implement NIST's important recommendations on these elements.

Finding 2: GSA continued to mislead its customer agencies after TTS suspended efforts to meet NIST IAL2 standards.

On June 24, 2021, FAS Deputy Commissioner/TTS Director Zvenyach internally announced the decision to suspend efforts to meet the biometric comparison requirement of the NIST standard, citing equity concerns with liveness detection. Zvenyach's internal Slack message to selected GSA personnel stated:

> Hey team, I have been hearing that there is still some ambiguity around TTS' position on liveness detection/PAD [Presentation Attack Detection] as an IAL2 proofing requirement. The position of TTS is that the benefits of liveness/selfie does not outweigh any discriminatory impact, and therefore should not be used as a proofing requirement.

However, Zvenyach did not notify customer agencies when TTS suspended efforts to implement selfies to meet the NIST biometric comparison requirement for IAL2 services.

Zvenyach told us that he did not know that Login.gov never met the NIST standard or that facial recognition was mandatory because he never explored the specific NIST provision for facial recognition. At the very least, Zvenyach should have recognized much earlier that Login.gov IAL2 services did not meet NIST standards. As the senior official over TTS and Login.gov, Zvenyach should have reviewed the standards to identify the implications of his decision to cease efforts to implement a selfie-check feature. Zvenyach was uniquely qualified to review those requirements with his prior GSA experience as the Executive Director overseeing Login.gov in 18F, and as an attorney trained in interpreting rules and requirements. Further, after identifying the implications for his decision, Zvenyach then should have ascertained which of the 22 Login.gov interagency agreements with GSA's customer agencies stated that they included IAL2 services, and alerted the affected agencies of their noncompliance with NIST standards.

GSA continued to withhold information from customer agencies about Login.gov's lack of biometric comparison capabilities until January 20, 2022, when the agency released its Equity Action Plan, required by Executive Order 13985, "Advancing Racial Equity and Support for Underserved Communities Through the Federal Government." That Plan provided:

> We will not deploy facial recognition, liveness detection, or any other emerging technology into production environments until rigorous review has given us confidence

> that they can be implemented equitably and without causing disproportionate harm to vulnerable populations.[29]

This statement linked the lack of a biometric comparison feature to equity concerns. It omitted any mention of the duration and nature of Login.gov's noncompliance with NIST's IAL2 requirements.

On January 28, 2022, *Wired* published an article stating that Login.gov "asks for selfies to check against photos of a person's ID."[30] The article relied on an assertion on GSA's Login.gov website that Login.gov used selfies for account verification. *Wired* retracted the statement about GSA's use of selfies on January 29, 2022, after GSA informed the publication that the Login.gov website was not accurate. After the article, [redacted] told us that Zvenyach stated he went through the IAL2 specifications and replaced [redacted] with [redacted] as Acting Director for the Login.gov division.

On February 3, 2022, seven months after Zvenyach's June 2021 internal announcement, GSA finally notified customer agencies that the IAL2 service included in their interagency agreements, for which they were paying, did not comply with NIST requirements published in SP 800-63-3. [31]

Although GSA had never met the NIST standards, Zvenyach's February 3, 2022, notifications to customer agencies cited his decision not to use facial recognition technology, a decision he actually made seven months earlier, as the basis for Login.gov not meeting the NIST standards:

> … although GSA has publicly discussed the use of "selfies" as part of an identity-proofing flow, we have made the decision not to use facial recognition, liveness detection, or any other emerging technology in connection with government benefits and services until rigorous review has given us confidence that we can do so equitably and without causing harm to vulnerable populations.
>
> When we executed our initial agreement with you, we indicated that Login.gov would be able to meet the IAL2 standards found in NIST 800-63-3. Our decision not to use facial recognition technology, however, means that Login.gov identity proofing services do not meet these standards at this time.

---

[29] GSA Executive Order 13985 Equity Action Plan, January 20, 2022, at pg. 10.

[30] https://web.archive.org/web/20220128225543/https://www.wired.com/story/irs-us-government-wants-selfies/

[31] Notification to one agency went out April 7, 2022.

This statement led customer agencies to believe that the decision to not use facial recognition technology due to equity concerns was the basis for Login.gov's noncompliance with IAL2 requirements, and that Login.gov had been compliant prior to that decision. Specifically, we found that multiple agencies' representatives thought the noncompliance began with Zvenyach's email notification. The notification did not reveal that Login.gov had never complied with SP 800-63-3.

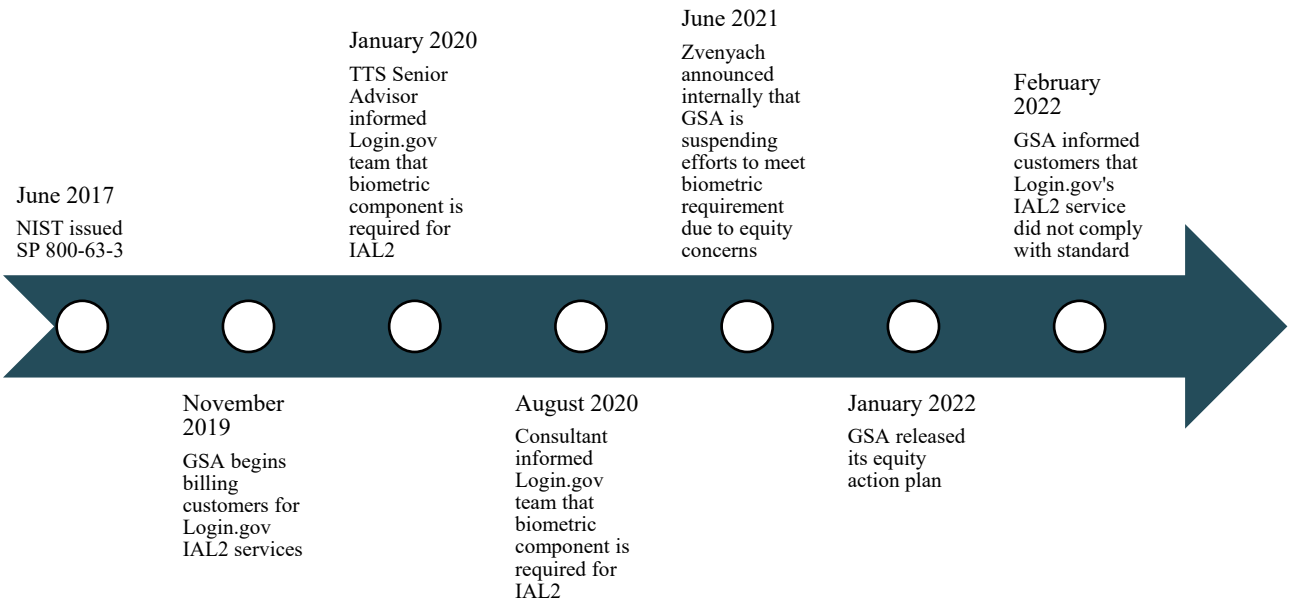
As late as April 27, 2022, Zvenyach told one customer agency:

> GSA will not deploy a remote biometric tool without it meeting GSA equity requirements under actual deployed conditions. While the planned equity study could be done towards the end of this year there is no certainty a vendor is found that meets the requirements.

When we asked what "the equity requirements" were, Zvenyach referred us to GSA's Equity Action Plan, not an external or official set of requirements.

Multiple GSA officials informed us that Login.gov did not meet the IAL2 standard because of Zvenyach's decision, announced internally on June 24, 2021, not to deploy facial recognition due to equity concerns. However, as reflected in Chart 1, the Login.gov services GSA sold to customer agencies had been noncompliant with NIST IAL2 standards long before GSA announced an equity-based rationale for the decision not to deploy facial recognition.

Chart 1. Timeline of noncompliance



We found emails from four customer agencies' representatives indicating their belief that, before Zvenyach's notification, they had been receiving NIST-compliant IAL2 services from GSA:

- "This is quite an issue. Thank you for letting us know. You are now stating that IAL2 is no longer available as of today? Was there any indication that you were going to stop the service prior [to] just announcing that you no longer provide it?" and "I will discuss with my leadership and stakeholders. As I see it, if it doesn't meet NIST 800-63A then it can't be used [as] IAL2. That would mean the level of service does change."

- "I apologize for the directness, but we really need to know if you all have already removed the facial recognition (selfie) part of the IAL2 flow. Our assumption is that you have already done this, but need to confirm." and "Thank you for the clarification. It sounds like we had a bit of a misunderstanding then. From what you are saying, since facial recognition was never implemented in production, our production systems were not in compliance at IAL2 with Login.gov since going live on Sept 30, 2021."

- "Login.gov will no longer support facial recognition to proof Identity Assurance. That means they are no longer compliant with IAL2 standards." and "We received the below notice from our colleague about the discontinuation of facial recognition on login.gov. I checked login.gov. Can you confirm that this change is now in effect?" and "All, this user has now received official word from Login.gov support that identity validation is not available for them and they should work with their partner agency (us) to provide an alternate login method. I reiterate how frustrating this is, since now, we're back to square one — at least a class of users who we need to maintain our own process for identity validation and login, which begs the question as to why we're using Login.gov at all."

- "You may have already provided it to [], but can you summarize more specifically how Login.Gov is not IAL2 compliant and also when you expect it will be compliant. We have been promoting the use of IAL2 solutions pretty heavily, so having a clear understanding of this is critical."

We interviewed representatives from the four agencies quoted above that all had current interagency agreements. All four agencies confirmed that they believed that they had been receiving SP 800-63-3 compliant IAL2 services from GSA. One customer agency official told us that Login.gov's noncompliance with the IAL2 standard created a greater risk of fraud for the customer agency. Another customer agency official told us that Login.gov's IAL2 noncompliance had an impact on the credibility of their program because the changes Login.gov made to the service gave stakeholders the impression that the customer agency did not perform their due diligence. An additional customer agency official told us that if they received non-complaint IAL2 services from Login.gov, the customer agency would be held responsible for allowing access to individuals at the wrong level.

We interviewed an official from one other agency that was not a Login.gov customer but participated in a Login.gov pilot that included IAL2 with a facial recognition component in 2020. One official from this agency informed us that they understood that if they became a Login.gov customer post-pilot, facial recognition would be included in the service. This customer agency ultimately decided that Login.gov did not meet their current needs, but continued to work with GSA to develop a solution with the understanding that Login.gov included a facial recognition component. GSA did not inform agency officials otherwise until February 2022.

In summary, from September 2018 to January 2022, Login.gov entered into 18 interagency agreements signed by the Assistant Commissioner of TTS based on templates that misrepresented that Login.gov's identity verification service *met* and/or were *consistent* with, the IAL2 requirements.[32]

Upon identifying that the interagency agreements misrepresented IAL2 as SP 800-63-3 compliant, GSA reviewed the agreements for other misrepresentations. As a result of their review, starting in February 2022, they found that Login.gov's default AAL2 setting was also not in compliance with the SP 800-63-3 standard. GSA sent email notifications informing customer agencies of the misrepresentation in March and April 2022. Between March 10 and March 15, 2022, GSA notified 51 Login.gov customers of Login.gov's AAL2 noncompliance; on April 7, 2022, it notified an additional agency of the noncompliance. Login.gov officials were able to remedy their AAL2 noncompliance by adjusting the settings in Login.gov to meet SP 800-63-3, but did not have the ability to meet IAL2 requirements.

GSA also updated the Login.gov website to reflect the current identity verification process that does not use selfies. As of July 21, 2022, Login.gov's website states in the Rules of Use section:

> After we have validated the identity evidence you provide to us, we verify that you are that person. We may do this by asking you to take a photo of yourself (a selfie) so that we can compare it to the photo identification, like driver's license or passport, that you provided (This feature is not currently enabled or required).[33]

[32] GSA billed 22 customer agencies for IAL2 services, but only 18 of those 22 customer agencies had interagency agreements with GSA that stated Login.gov met and/or was consistent with the IAL2 requirements.

[33] https://login.gov/policy/rules-of-use/

GSA also updated the Login.gov website to state:

> Login.gov *adheres* to the latest security standards established by top security organizations such as the National Institute of Standards and Technology, the Cybersecurity National Action Plan and the Federal Acquisition Service. (Emphasis added.) [34]

On August 16, 2022, the GSA Administrator announced the Zvenyach's departure from GSA, effective September 9, 2022. Effective November 21, 2022, [redacted] resigned his federal position at GSA.

Finding 3. GSA billed customer agencies for IAL2 services not provided.

Starting in 2019, Login.gov began charging customer agencies for IAL2 services that did not meet the requirements of SP 800-63-3. GSA billed 22 customer agencies for the non-existent Login.gov IAL2 services. Four of these customer agency interagency agreements were for IAL1 services, but GSA still billed the agencies for IAL2 services. According to the TTS Operations Division, Login.gov has billed IAL2 customers more than $10 million for services through May 2022 (see Table 1).[35] Moreover, even after notifying customer agencies in February 2022 that their services were not compliant with NIST IAL2 standards, Login.gov continued to bill agency customers for IAL2 services.

Table 1. IAL2 Billings

Fiscal Year	Billed
2020	$459, 877
2021	$4,288,990
2022 through May 2022	$5,311,387
Total	**$10,060,254**

The TTS Business Operations Director stated that because GSA had never billed customer agencies the full amount required for Login.gov to be fully cost recoverable, the non-compliant

[34] https://login.gov/who-uses-login/

[35] The Business Operations Director said that the Operation Division facilitates Login.gov's Interagency Agreement signing process and manages Login.gov's billing process. The billed amounts include IAL2 identity verification fees, IAL2 platform fees, and authentication fees for both IAL1 and IAL2. Login.gov did not differentiate between IAL1 and IAL2 authentication fees in their billings to customer agencies, nor within their own billing records.

services the agencies received were still worth more than the agencies were billed. As a result, customer agencies did not receive any remedy for the improper IAL2 billings.

TTS' rationale ignores the possibility that, had they known the services did not include NIST compliant IAL2 services, agencies might not have entered into interagency agreements with GSA at all. The rationale also overlooks potential costs to the customer who must choose between the costs of researching and implementing a new identity verification platform or using a platform that does not meet their requirements.

Finding 4. GSA made inaccurate statements about Login.gov's compliance with IAL2 to obtain TMF funds.

GSA misled the Technology Modernization Board in securing funding for Login.gov. The Federal Chief Information Officer and six federal government IT executives make up the board. The board provides awards from the Technology Modernization Fund (TMF) to agencies to help them improve, retire, or replace existing systems. The TMF process allows agencies to submit IT-related proposals for the board to review and consider through a two-phased approval process.[36] The mission of the TMF is to enable agencies to reimagine and transform the way they use technology to deliver their mission and services to the American public in an effective, efficient, and secure manner.

In September 2021, GSA submitted a proposal seeking TMF funds for use on Login.gov, and ultimately received approximately $187 million covering the years 2022 through 2025. The TTS Business Operations Director informed us that Login.gov received $187 million from the TMF for three purposes: 1) to accelerate the adoption of Login.gov services to help Login.gov achieve economies of scale, 2) to ensure that Login.gov is equitable, and 3) to increase cybersecurity and antifraud capacities. The Business Operations Director said that TTS would use TMF funds to cover Login.gov charges for partner agencies if the agencies agree to an enterprise-level adoption of Login.gov.[37] In May 2022, The TTS Business Operations Director told us that TTS had already exhausted all fiscal year 2022 TMF funds that they had allocated to cover partner agencies' no-cost agreements, and that ten partner agencies were receiving TMF subsidized Login.gov services.

[36] https://tmf.cio.gov/

[37] Enterprise-level adoption refers to customer agencies who establish an interagency agreement for Login.gov agency-wide, making services available to all components.

In the proposal for the TMF funding, GSA stated:

> …[l]ogin.gov provides authentication and identity verification shared services, in accordance with M-19-17, to provide access to benefits and services to the correct users.

And:

> Login.gov is currently used in production and complies with NIST's 800-63-3 standard for strong authentication (AAL2) and identity verification (IAL2).[38]

[redacted], Zvenyach, former GSA Chief Financial Officer Gerard Badorrek, and GSA Chief Information Officer David Shive signed the TMF proposal. However, as discussed above, Login.gov did not comply with SP 800-63-3, despite the assertions included in the TMF proposal that it did.

Shive, who also holds the role of Technology Modernization Board member, told us that based on his discussions with [redacted] shortly after the *Wired* article was published on January 28, 2022, he did not believe that the Login.gov team intentionally concealed the truth about the program's noncompliance with SP 800-63-3. Shive stated that if he thought Login.gov officials were misleading him then he would have intervened.

Subsequently, on February 7, 2022, Deputy Administrator Katy Kale notified the Technology Modernization Board through a letter stating that Login.gov's TMF proposal made statements "that *could be interpreted* to say Login.gov's service meets NIST guidelines for identity verification." (Emphasis added.) In fact, Login.gov identity proofing services did not meet the IAL2 standard at that time and, as quoted above, GSA expressly represented that Login.gov "complies with NIST's 800-63-3 standard" for both IAL2 and AAL2.

Kale's notification attributed Login.gov's IAL2 noncompliance to their decision not to use facial recognition technology until they are confident it is equitable. However, as discussed in Finding 2, Login.gov's noncompliance with the IAL2 standard preceded GSA's decision not to use facial recognition technology. Furthermore, the TMF proposal and the interagency agreements said that Login.gov met, was consistent with, or complies with the standard, leaving little space for interpretation.

[38] The proposal also noted that Login "requires more than its current identity proofing to provide equitable access" and "… the IAL2 specification … is already being revised to address critical issues in equity and usability."

Finding 5. FAS shares the responsibility for the misrepresentations TTS and Login.gov made to GSA's customer agencies.

The misrepresentations by FAS components to Login.gov customer agencies and the Technology Modernization Board show a failure of leadership at the Login.gov level and the TTS level. Our interviews found that Login.gov operated independently without adequate oversight and management controls from TTS. FAS permitted this and ultimately is responsible for what happened and for any consequent harm to TTS's credibility with agencies that might seek TTS services.

FAS exercised inadequate oversight and management controls over Login.gov's day-to-day operations. Office of Management and Budget Circular A-123 "Management's Responsibility for Enterprise Risk Management and Internal Control," July 15, 2016, states:

> Management's responsibility is to develop and maintain effective internal control that is consistent with its established risk appetite and risk tolerance levels. In addition, management is responsible for establishing and integrating internal control into its operations in a risk-based and cost beneficial manner, in order to provide reasonable assurance that the entity's internal control over operations, reporting, and compliance is operating effectively.[39]

Hashmi, appointed as FAS Commissioner in January 2021, acknowledged that when TTS merged into FAS in 2017, FAS did not make TTS a part of FAS's organizational culture, with the consequence that FAS lacked understanding of and visibility over TTS representations. FAS allowed TTS's culture to continue unchecked without incorporating FAS management controls over TTS, and deliberately allowed 18F (where Login.gov began) to operate distinctly to encourage innovation. As a consequence, even though TTS became a part of FAS five years ago, TTS worked independently of the FAS organization and each project team operated independently without sufficient collaboration.

Hashmi told us that TTS's failure is rooted in its historic 18F culture that considered oversight burdensome and believed it did not have to align its practices with other components. Previous OIG reports on 18F activities provide some insight into what Hashmi calls the 18F culture. One

[39] https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2016/m-16-17.pdf

report found that 18F operated as a "separate unit with a start-up mentality" and "routinely disregarded and circumvented fundamental GSA information security policies."[40]

According to Zvenyach, the Login.gov team retained its own significant autonomy over program decisions and choices regarding features, communication with the public, and communication with customer agencies. Additionally, he found a culture wherein teams believed they did not need to escalate decisions to leadership or that escalating was worthwhile. As one person working in Login.gov told us, "no one was at the wheel" for IAL2 decisions, enforcement, responsibility and accountability. There also were no clear policies, management controls, or checks and balances for Login.gov. As the FAS Commissioner, Hashmi understood this to be the 18F/TTS culture.

According to Hashmi, this autonomy, combined with business pressures for Login.gov to close deals, increase revenue, and achieve cost recovery, led the Login.gov team to create their own understanding of the IAL2 standard in practice. Hashmi told us that some internal TTS controls were missing, broken, or not followed. Hashmi also said Login.gov officials needed controls to identify gaps in management hierarchy protocols, which did not exist. Hashmi stated that since January 2022, FAS has addressed the absence of management controls over financial planning, cost planning, procurement, and program management and more closely aligned TTS controls with FAS controls.

We also found a lack of controls when we asked for written policies and procedures governing Login.gov, and TTS officials only could direct us to the Login.gov public facing website and GSA IT policies, none of which contain formal management controls. Multiple officials told us that they were not aware of any controls, policies, or desk guides for Login.gov. We identified the same issue in our 2016 report, *Evaluation of 18F*, where the agency was unable to locate and provide documentation to support billings to customer agencies.[41]

Hashmi also acknowledged concerns that TTS's underlying system for records management may not be able to meet National Archives and Records Administration's documentation requirements due to the failure to document significant decisions concerning the operations of Login.gov. All federal agencies are required to make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and

[40] GSA OIG report JE17-002, *Evaluation of 18F's Information Technology Security Compliance*, February 21, 2017, at pgs. 8, 9. For other reports on 18F, see *Evaluation of 18F*, JE17-001, October 24, 2016, and *Management Alert Report, GSA Data Breach*, JE16-004, May 12, 2016. For a discussion of 18F's history, see *Investigation of Whistleblower Reprisal Complaint*, June 2017.

[41] *Evaluation of 18F*, October 24, 2016, Report Number JE17-001.

essential transactions of the agency. GSA must manage these records according to applicable authorities.[42]

Hashmi told us that the Login.gov team's core failure was the lack of transparency to customers. However, we found FAS's core failure was greater. Knowing the history and culture of TTS and 18F, FAS maintained the status quo when TTS became a part of FAS, effectively ignoring OMB's Circular A-123 caution to establish management controls, and gave TTS the independence and lack of oversight that empowered Login.gov to mislead customer agencies.

Conclusion

Login.gov has never met the technical requirements for identity proofing and authentication of SP 800-63-3 for IAL2. At multiple points starting in 2019, Login.gov officials should have notified customer agencies that Login.gov did not comply with IAL2 requirements in SP 800-63-3. However, Login.gov did not notify their customer agencies until February 3, 2022, after a *Wired* article reported that Login.gov used selfies for verification. Before then, Login.gov not only portrayed publicly that it was compliant with IAL2 requirements, but also misinformed customer agencies through interagency agreements stating that they *met* and/or were *consistent* with the IAL2 requirements.

Furthermore, Login.gov continued to bill customer agencies for IAL2 services that did not comply with SP 800-63-3 and, therefore, are not IAL2 services. In addition, Login.gov inaccurately asserted that it met SP 800-63-3 when it applied for TMF funding, which they received.

Finally, FAS exercised inadequate oversight and management controls over Login.gov's day-to-day operations, and thus bears responsibility for TTS's and Login.gov's derelictions. FAS's failure to establish management controls allowed TTS's hands-off culture to continue unchecked, and empowered Login.gov to mislead customer agencies.

We are providing this report to GSA for appropriate disciplinary action. In addition, we provide the following recommendations.

[42] The Federal Records Act of 1950, as amended (44 U.S.C §3101 and §3102).

Recommendations

The Federal Acquisition Service Commissioner should:

1. Establish adequate management controls over TTS.
2. Ensure adequate documentation of policies, decisions, procedures, and essential transactions involving TTS programs, including Login.gov, and records management in accordance with GSA standards.
3. Implement a comprehensive review of Login.gov billings for IAL2 services.
4. Establish a system for internal reviews of TTS programs to ensure that they comply with relevant standards.
5. Adopt a policy to clearly notify each customer agency seeking identity and authorization assurance services whether Login.gov meets all applicable NIST published standards and the services specified in the interagency agreements.

Appendix 1: Objective, Scope, and Methodology

On April 1, 2022, the General Service Administration (GSA) Office of Inspector General (OIG) Office of Inspections initiated an evaluation of GSA's Technology Transformation Services (TTS) Login.gov services. The objective of the Login.gov evaluation include, but not limited to, assessments of transparency with regard to National Institute of Standards and Technology (NIST) compliance discrepancies, system security vulnerabilities, and oversight and management controls of Login.gov and the Technology Transformation Services.

The evaluation team performed the evaluation from April 2022 to February 2023. The evaluation covered the Login.gov program during the period May 2016 through December 2022. During the evaluation, we:

- Researched laws, rules, regulations, and other federal guidance on identity assurance;
- Researched relevant audits and inspections conducted by GSA OIG, the U.S. Government Accountability Office, and other federal agencies;
- Reviewed the Interagency Agreements related to Login.gov billed services for NIST IAL2 and AAL2;
- Reviewed for internal guidance or policies governing Login.gov management controls for decisions processes, communication, and documentation;
- Interviewed personnel at GSA's TTS and Login.gov official staff;
- Interviewed officials from external customer agencies;
- Interviewed officials from National Institute for Science and Technology concerning SP 800-63 and related publications; and
- Reviewed email documentation.

We conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency, *Quality Standards for Inspection and Evaluation*, issued December 2020.

Appendix 2: Management Comments

DocuSign Envelope ID: D7B6D4CE-D007-45A1-8EC7-CA75C24F1266

GSA

Federal Acquisition Service

March 6, 2023

MEMORANDUM FOR: Patricia D. Sheehan
Assistant Inspector General for Inspections
Office of Inspector General (JE)

FROM: Sonny Hashmi
Commissioner
Federal Acquisition Service (Q) Sonny Hashmi

SUBJECT: Response to Draft Report – GSA Misled Customers on Login.gov's Compliance with Digital Identity Standards (JEF22-004-000)

Thank you for the Office of Inspector General's (OIG) evaluation of Login.gov. GSA appreciates the OIG's thorough review of this matter, and concurs with the OIG's findings and recommendations. Earning and maintaining the American people's trust through transparent and accountable actions is one of the Agency's highest priorities. Accordingly, as detailed below, GSA is committed to bolstering accountability and transparency, and over the past year has put additional controls in place to ensure that there is adequate oversight of Login.gov.

In late January 2022, GSA officials learned that Login.gov did not meet the Identity Assurance Level 2 (IAL2) standard found in NIST SP 800-63-3, despite assertions to the contrary. In response, GSA quickly took a number of remedial actions to ensure that Login.gov was accurately describing its capabilities. First, in early February 2022, GSA notified customers and relevant stakeholders about the issue, including the OIG. Then, in the following days and weeks, GSA updated public facing materials on the Login.gov website and amended interagency agreements with client agencies.

GSA also quickly launched a broader internal review to better understand the extent of the issue. That review uncovered a number of troubling findings—including that multiple Login.gov employees knew (potentially as early as 2019) that Login.gov was not in compliance with NIST SP 800-63-3 for IAL2. Accordingly, GSA referred the potential employee misconduct matter to the OIG.

In addition to the actions above and in response to the findings of our internal review, we have already taken a number of actions to ensure that the issue does not recur and

1

that Login's capabilities will be accurately conveyed to users, agency customers, and members of the public:

Accountability—Given that employees misled customer agencies about Login.gov's compliance with NIST standards, GSA leadership has acted to hold appropriate individuals accountable. In February 2022, the then-Director of Login.gov was reassigned internally and GSA hired a new Director to oversee the program. Additionally, upon conclusion of the internal review, GSA initiated an employee misconduct inquiry. Disciplinary actions are proceeding in accordance with GSA protocols and appropriate due process.

Oversight—To ensure that there is adequate oversight of and support for Login.gov, I have directed a number of reviews and GSA has expanded support for the Login.gov program. First, I directed the new Login.gov Director to conduct a top-to-bottom review of the program in order to determine where improvements can be made. I have also initiated a review of TTS financial operations, including existing financial management controls. Recommendations from both of these reviews will be incorporated into the overall FAS management control and oversight corrective action plan. Further, in May 2022, GSA created a new Technology Law Division within GSA's Office of the General Counsel, which will provide dedicated legal services to GSA's technology-focused components, with an emphasis on advising on technology-related standards. Together, these efforts will help to ensure, among other things, that GSA develops adequate oversight and management controls over Login.gov's operations.

Transparency—In June 2022, GSA created an executive steering committee for Login.gov to provide oversight and support for existing leadership, including guidance from the United States Digital Service, the Office of Management and Budget, and the Office of the Federal Chief Information Officer. In addition, to ensure that Login.gov's communications are accurate and transparent, GSA has been providing regular partner updates on the program's compliance status, continues to ensure that IAAs are accurate, and is committed to proactively and regularly communicating with partners about Login.gov's capabilities.

GSA is committed to developing a secure, scalable, trusted, and accessible authentication and identity verification solution that reduces burden and risk for our agency partners, and that helps the American people access the government services they need in a seamless and secure manner while advancing equity, protecting privacy, and preventing fraud. Toward that end, an equity study is underway, which will help GSA better understand the current technological barriers to equitable remote identity-proofing services for the public (including remote biometric comparison with liveness detection and other approaches) and will inform potential next steps. In the meantime, Login.gov will continuously evolve and improve its fraud program and capabilities.

Thank you again to you and your team for your thorough review. GSA fully concurs with the OIG recommendations. We look forward to submitting a corrective action plan that will help to further address the issues identified in your report.

OFFICE OF INSPECTOR GENERAL

U.S. General Services Administration

For media inquiries

OIG_PublicAffairs@gsaig.gov

(202) 273-7320

get CONNECTED

subscribe to the MAILING LIST

LinkedIn

REPORT FRAUD, WASTE, AND ABUSE

www.gsaig.gov/hotline